Mae 234 – Introduction to Cryptography

Dr. David L. Wehlau

Royal Military College of Canada
Kingston, Ontario

Chapter 1

Overview of Cryptography

1.1 Secure Communications

There are terms that are used in the field of cryptography

Definition 1.1

cryptology is the study of communications over nonsecure channels and related problems

cryptography is the process of designing systems to communicate over nonsecure channels

cryptanalysis is the breaking of such systems

The basic communication scenario is this. There are two parties, Alice and Bob, who want to communicate with each other. There is a third party, Eve, who is a potential eavesdropper.

Alice wants to send a message, called the *plaintext*, to Bob. She encrypts the message using a method prearranged with Bob. The encrypted message that Bob receives is called the *ciphertext*, which he changes back to the plaintext, by means of a *key*.

Eve may want to

1. Read the message
2. Find the key and read all messages encrypted
3. Corrupt Alice's message in order to mislead Bob
4. Impersonate Alice while communicating to Bob

In cases 1 and 2, the third party is sometimes called Oscar (O for *observer*) instead of Eve. In cases 3 and 4, the third party is called Mallory (M for *malicious*).

1.1.1 Possible Attacks

1. **Ciphertext only** Eve only has a copy of the ciphertext
2. **Known Plaintext** Eve has a copy of a ciphertext and the corresponding plaintext.
   (a) Eve has an encrypted press release, which is published in decrypted form the next day.
   (b) Alice starts all of her messages to Bob with the same text, such as "Dear Bob,"
   (c) Sending the same message repeatedly: "Nothing new to report."
3. **Chosen Plaintext**: Eve has access to the encryption machine, which she uses to encrypt plaintexts. She can then (try to) use the resulting ciphertexts to deduce the key.
4. **Chosen Ciphertext**: Eve has access to the decryption machine, which she uses to decrypt ciphertexts. She can then (try to) use the resulting ciphertexts to deduce the key.

Kerckhoff's Principle: In assessing the security of a cryptosystem, one should always assume the enemy knows the method being used.

- It is too easy for Eve to obtain this info
  - Encryption/decryption machine's can be captured.
  - Defections/captures
- Don't want to change the whole system when Eve learns this. It is easier to change the key.
- Analyze Eve's difficulty in determining the key, assuming she knows the method.

1.1.2 Symmetric vs. Public Key Algorithms

Encryption methods can be divided into two categories, *symmetric key* and *public key*.

Definition 1.2 1. *symmetric* or *private key*: both Alice and Bob know both encryption and decryption keys (possibly they are the same)

All of the systems before the 1970s were symmetric. Eg. DES, AES (Rijndael), historical methods

2. *asymmetric* or *public key*: Encryption key is public, but decryption key is private (or vice-versa). This means that anyone can encrypt, but only the receiver (Bob) can decrypt.

Public key systems have the added advantage of security, but this comes at a cost. Algorithms can be computationally intensive. ie. it takes a lot of computing power to encrypt and/or decrypt. Eg. RSA, discrete logarithms, El Gamel.

Symmetric ciphers are divided into two types,

Definition 1.3
1. *stream ciphers*: the data are fed into the encryption algorithm in small pieces (bits or characters), and the output is produced in corresponding small pieces.
2. *block ciphers*: blocks of plaintext (in bits or characters) are encrypted into blocks of ciphertext.

1.1.3 Key Length

One important property of a cryptographic algorithm is its security. Most algorithms employ (numerical) keys. One way of cracking the key is to simply try every key. This is known as a *brute force attack* or *exhaustive attack*.

The length of the key is related to how long it will take to check all keys.

If the key is 16 bits, then there are $2^{16} = 65536$ possible keys.

The DES algorithm has a 56-bit key and thus has $2^{56} \approx 7.2 \times 10^{16}$ possible keys.

A key length of 30 digits (≈ 150 bits) gives 10^{30} possible keys. A computer which can check 10^9 keys per second (1 year is $\approx 3 \times 10^7$ seconds) would take more than (3×10^{13}) years, which exceeds the predicted age of the universe.

Note: a simple substitution has $26! \approx 4 \times 10^{26}$ keys, but is easily broken, while DES has **much** fewer keys ($\approx 7.2 \times 10^{16}$), but is very hard to break.

1.2 Cryptographic Applications

1. **Confidentiality**: Eve should not be able to read Alice's messages to Bob.
2. **Data Integrity**: Bob should know that Alice's message has not been changed.
3. **Authentication**: Bob wants to be sure that only Alice could have sent the message he received. This includes identification schemes and password protocols (in which case, Bob is a computer).

4. **Non-repudiation**: Alice cannot claim she did not send the message (nor can she claim that Bob sent the message). Important in e-commerce: customer cannot deny the authorization of a purchase.

5. **Key establishment**: Alice and Bob need to communicate what keys to use to communicate with each other. Important when large quantities of data are to be exchanged. Public key is inefficient for large quantities, so private key must be used. How do Alice and Bob establish a key securely?

6. **E-commerce**: carry out secure transactions over open channels

7. **Games**: Eg. dealing cards over the internet.

1.3 Conventions

1. plaintext is given in lower case.

   ciphertext is given in UPPER CASE.

2. In many encryption schemes, we map the letters of the alphabet with the numbers $0, \cdots, 25$ according to their position in the alphabet, starting with 0 (this is probably different from what you're used to),

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

3. Spaces and punctuation are omitted. (Spaces give too much information about the text.)

Chapter 2

Classical Cryptosystems

2.1 Caesar Cipher

The Caesar Cipher is also called a *shift cipher*.

1. The key is a number $\tau \in \mathbb{Z}/26\mathbb{Z}$.
2. To encrypt, map the number n to $n + \tau$ (n is the number corresponding to the letter in plaintext).
3. To decrypt, map the number m to $m - \tau$ (m is the number corresponding to the letter in ciphertext)

Addition and subtraction are done modulo 26. If $n + \tau > 25$, we subtract 26. Similarly, if $n - \tau < 0$ we add 26.

Example 2.1 Suppose that we want to send the plaintext

cryptography

using a Caesar cipher with key $\tau = 3$.

First we map the letters in the plaintext to the corresponding numbers,

$$c \mapsto 3, r \mapsto 17, y \mapsto 24, \ldots, h \mapsto 7, y \mapsto 24$$

to get the sequence $(3, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24)$ Now we add $\tau = 3$ to each number in this sequence to get

$$(6 + 3, 20 + 3, 24 + 3, \ldots) = (6, 20, 27, 18, 22, 17, 9, 20, 3, 18, 10, 27)$$

Two entries are greater than 25, so we subtract 26 from these entries to get

$$(6, 20, 1, 18, 22, 17, 9, 20, 3, 18, 10, 1)$$

Mapping theses numbers to the corresponding letters, we get the ciphertext

$$GUBSWRJUDSKB$$

To decrypt, we reverse this process. Letters $\mapsto$ numbers

$$GUB\ldots \mapsto (6, 20, 1, \ldots)$$

Subtract $\tau = 3$

$$(6-3, 20-3, 1-3, \ldots) = (3, 17, -2, \ldots)$$

Add 26 to negative entries

$$(3, 17, -2+26, \ldots) = (3, 17, 24, \ldots)$$

Numbers $\mapsto$ letters

$$cry\ldots$$

This system is simple enough that we didn't need to go through all of these details. Instead, the ciphertext for each letter can be found by shifting to the right by $\tau = 3$ places in the alphabet, wrapping around to the beginning of the alphabet if we reach the end. The plaintext can be found by shifting to the left by $\tau = 3$.

2.1.1 Attacks on Caesar Cipher

1. **Ciphertext only attack**: There are two possible methods.
   (a) **Exhaustive search**: There are only 26 possible keys τ (actually 25, since $\tau = 0$ means plaintext=ciphertext.) Check each one until something makes sense. (It's unlikely that two different keys will yield a meaningful plaintext)
   (b) **Frequency analysis**: In an average text of English, the letters aren't distributed evenly. Some letters appear more than others. Examine the ciphertext for letters that appear most frequently.

a	b	c	d	e	f
0.082	0.015	0.028	0.043	0.127	0.022
g	h	i	j	k	l
0.020	0.061	0.070	0.020	0.008	0.040
m	n	o	p	q	r
0.024	0.067	0.075	0.019	0.001	0.060
s	t	u	v	w	x
0.063	0.091	0.028	0.010	0.023	0.001
y	z				
0.020	0.001				

   Frequency analysis may fail if the plaintext does not contain a common letter.

2. **Known Plaintext** Knowing 1 letter and its ciphertext is enough to find τ. For example, if you know that t $(= 19)$ encrypts to $D(= 3)$, you know that $19 + \tau = 3$. Therefore, $\tau = 3 - 19 = -16 \equiv 10 \mod 26$.

3. **Chosen Plaintext** Choose $a(= 0)$. It is encrypted to $0 + \tau = \tau$, which is the key.

4. **Chosen Ciphertext** Choose $A(= 0)$. It is decrypted to $0 - \tau = -\tau$, the negative of the key.

2.2 Affine Ciphers

Choose integers α and β such that $\gcd(\alpha, 26) = 1$.

- **Encryption key**: (α, β).
- **Encryption function**: x maps to $\alpha x + \beta$ (reduced modulo 26).
- **Decryption function**: To decrypt, we need to solve

$$y = \alpha x + \beta \quad \text{for} \quad x$$

modulo 26.

Example 2.2 Use an affine cipher with key $(9, 2)$ to encrypt the word "affine".

Solution. The encryption function is $x \mapsto 9x + 2$

$$a \leftrightarrow 0 \mapsto 9(0) + 2 = 2 \mapsto C$$
$$f \leftrightarrow 5 \mapsto 9(5) + 2 = 47 \equiv 21 \mod 26 \mapsto V$$
$$f \leftrightarrow \cdots V$$
$$i \leftrightarrow 8 \mapsto 9(8) + 2 = 74 \equiv 22 \mod 26 \mapsto W$$
$$n \leftrightarrow 13 \mapsto 9(13) + 2 \equiv 15 \mod 26 \mapsto P$$
$$e \mapsto 9(4) + 2 \equiv 12 \mod 26 \mapsto M$$

So

$$affine \mapsto CVVWPM$$

□

Example 2.3 Find the decryption function for the previous example.

Solution. To decrypt, we need to solve

$$y = 9x + 2$$

for x. This is easy enough in ordinary arithmetic, but we need to solve it modulo 26. First,

$$y - 2 = 9x$$

Normally, we would divide by 9. Instead we multiply by the inverse of 9,

$$x = 9^{-1}(y - 2)$$

In ordinary arithmetic, the (multiplicative) inverse of the number 9 is $9^{-1} = \frac{1}{9}$. The number $\frac{1}{9}$ has the property $9(\frac{1}{9}) = 1$. This property is what defines the inverse.

In arithmetic modulo 26, the situation is similar. If a is the multiplicative inverse of 9, then a has the same property that $9a = 1$, except that this equation must hold modulo 26. So if 9 has a multiplicative inverse[1], then there is a number a between 0 and 25 such that $9a \equiv 1 \mod 26$. In that case $a = 9^{-1}$. There are methods for finding multiplicative inverses modulo n (if they exist), but for now, a brute force approach will do. We simply multiply 9 by all numbers until we find one that reduces to 1 mod 26.

$$0(9) = 0 \not\equiv 1 \mod 26$$

$$1(9) = 9 \not\equiv 1 \mod 26$$

$$2(9) = 18 \not\equiv 1 \mod 26$$

$$3(9) = 27 \equiv 1 \mod 26$$

Since $3(9) \equiv 1 \mod 26$, the $9^{-1} = 3 \mod 26$.

Therefore, $x = 3(y - 2)$ (modulo 26). □

Example 2.4 Use the decryption function to decrypt the ciphertexts N and V

Using the formula $x = 3(y - 2)$ and reducing modulo 26, *Solution.*

$$N \mapsto 13 \mapsto 3(13 - 2) = 33 \equiv 7 \mod 26 \mapsto h$$

$$V \mapsto 21 \mapsto 3(31 - 2) = 57 \equiv 5 \mapsto 26 \mapsto f$$

□

[1]Not all integers modulo n have a multiplicative inverse

Example 2.5 Suppose that we use the key $(\alpha, \beta) = (13, 4)$. If we apply the affine cipher to the plaintexts "input" and "alter", we get

$$input \mapsto ERRER$$

$$alter \mapsto ERRER$$

Two different plaintexts map to the same ciphertext. This is a problem, since there would be no way to tell what the intended plaintext was if the ciphertext is ERRER.

Note that $\gcd(13, 26) = 13 \neq 1$. Thus, if the condition $\gcd(\alpha, 26) = 1$ must be satisfied, otherwise the system could fail.

Note: There are 12 choices for α (no even numbers, no multiples of 13, need only consider $1 \leq \alpha \leq 25$). There are 26 choices for β (β can be anything between 0 and 25). Thus, the keyspace has size $12 \times 26 = 312$.

2.2.1 Attacks on Affine Ciphers

1. **Ciphertext only**: Use brute force or frequency analysis.
2. **Known plaintext**: Usually 2 letters (along with the corresponding ciphertext) suffice

   Example 2.6 Suppose that

   $$if \mapsto PQ$$

   $$8, 5 \mapsto 15, 16$$

   Since $x \mapsto \alpha x + \beta$ for any plaintext letter x, for some numbers α and β, we have

   $$\begin{array}{rcl} 8\alpha + \beta & = & 15 \mod 26 \\ 5\alpha + \beta & = & 16 \mod 26 \\ \hline 3\alpha & = & -1 \mod 26 \end{array}$$

   We saw in another example that 3 and 9 are inverses of each other modulo 26. Therefore, we multiply this equation by 9 to get $\alpha = -9 \equiv 17 \mod 26$ and so $\beta = 15 - 8\alpha = 9 \mod 26$. Thus, the key is $(\alpha, \beta) = (17, 9)$.

   Example 2.7 Suppose that

   $$go \mapsto TH$$

   $$6, 14 \mapsto 19, 7$$

   yielding equations

$$\begin{aligned} 6\alpha + \beta &= 19 \mod 26 \\ 14\alpha + \beta &= 7 \mod 26 \\ \hline -8\alpha &= 12 \mod 26 \end{aligned}$$

Therefore,

$$-4\alpha = 6 \mod 13$$

But $-4 \equiv 9 \mod 13$, so this is

$$9\alpha = 6 \mod 13$$

So

$$\alpha = 3(6) \equiv 5 \mod 13$$

Thus, $\alpha \equiv 5$ or $18 \mod 26$.

Therefore, $\beta = 15 \mod 26$ (plugging either of $\alpha = 5$ or $\alpha = 8$ into either of the original equations), so the key is $(\alpha, \beta) = (5, 15)$ or $(\alpha, \beta) = (18, 15)$, but $\gcd(18, 26) = 2 \neq 1$, so the key must be $(5, 15)$.

Information about the key can be obtained even if only 1 letter of plaintext and its ciphertext is known.

For example, suppose we know that $g(= 6)$ in plaintext corresponds to $T(= 19)$ in ciphertex, then we know that $6\alpha + \beta \equiv 19 \mod 26$. There are 12 possibilities for α and each gives a corresponding β. The correct key can be found by an exhaustive search.

3. **Chosen plaintext**: Choose ab as the plaintext. Then,

$$a \leftrightarrow 0 \mapsto \alpha(0) + \beta = \beta$$

$$b \leftrightarrow 1 \mapsto \alpha(1) + \beta = \alpha + \beta$$

Example 2.8 Suppose that $0 \mapsto 2$ and $1 \mapsto 11$.

Then $\beta = 2$ and $\alpha + \beta = 11$. Thus $\alpha = 11 - \beta = 2$. Thus the key is $(\alpha, \beta) = (9, 2)$.

4. **Chosen ciphertext**: Decrypt AB:

$$A \leftrightarrow 0 \mapsto \gamma_1$$

$$B \leftrightarrow 1 \mapsto \gamma_2$$

(The ciphertext letters A and B are decrypted to the plaintext letters γ_1 and γ_2 (or their numerical equivalents)) Since γ_1, γ_2 are the plaintext of $A, B(= 0, 1)$,

$$\begin{aligned} \alpha\gamma_1 + \beta &= 0 \\ \alpha\gamma_2 + \beta &= 1 \end{aligned}$$

We can solve for α and β to find the encryption key as follows.

By the first equation, $\gamma_1 = -\beta\alpha^{-1}$.

By the second equation, $\gamma_2 = \alpha^{-1} - \underbrace{\beta\alpha^{-1}}_{-\gamma_1}$, so $\alpha^{-1} = \gamma_2 - \gamma_1$.

Since, $x = \alpha^{-1}(y - \beta) = \underbrace{\alpha^{-1}}_{\gamma_2-\gamma_1} y - \underbrace{\alpha^{-1}\beta}_{\gamma_1}$, we can decrypt using $x = (\gamma_2 - \gamma_1)y + \gamma_1$.

2.3 Substitution Cipher

The Caesar cipher and the Affine Cipher are both special cases of a *monoalphabetic substitution* cipher:

Each plaintext letter is always encrypted to the same ciphertext letter.

Each ciphertext letter is always decrypted to the same plaintext letter.

In other words, a permutation of the alphabet is chosen and applied to the plaintext. The key is the chosen permutation.

Caesar cipher: $n \to n + \tau \mod 26$

Affine cipher: $x \mapsto \alpha x + \beta \mod 26$ (Caesar is a special case, with $\alpha = 1$.)

(In both cases, the ciphertext of a letter in plaintext is given by a formula, but this need not be the case.)

2.3.1 Attacks on substitution cihpers

1. **Ciphertext only** Any substitution cipher is vulnerable to attacks based on frequency analysis.
   (a) Letters that occur the most frequently in the ciphertext probably correspond to letters that occur frequently in an average English text.
   (b) This can be used to guess what the more frequently occurring letters correspond to. This may not be enough if the frequencies in the plaintext aren't the same as an average English text.
   (c) Use analysis of *digrams*, that is, two letter sequences of letters.
   - As with letters, digrams are not evenly distributed: some occur more frequently than others.
     For example, *th* is the most common digram. If *BN* occurs frequently in a text, then probably
     $$B \leftrightarrow t \qquad \text{and} \qquad N \leftrightarrow h$$

- Around 80% of the letters preceding the letter n are vowels. Thus, if we know which ciphertext letters are vowels, we can look for letters that are commonly preceded by vowels. One of these is probably the ciphertext of n.
- rn occurs for more frequently than rn. Suppose we know that one of A,B corresponds to r and the other corresponds to n. If AC occurs more frequently than CA then probably
$$AC \leftrightarrow rn$$
so
$$A \leftrightarrow r \qquad \text{and} \qquad C \leftrightarrow n$$
- After the most frequent letters have been decrypted, the remainder can be filled in by educated guessing and knowledge of the language
For example, if you see

B	A	Y	B	N
t	r		t	h

you could guess that $Y \leftrightarrow u$, giving the plaintext *truth*

2. **Known plaintext** If each letter of the alphabet occurs in the plaintext, then the key can be found.

   If not all letters of the alphabet occur, but another ciphertext is known (without the plaintext) then, techniques from the ciphertext only attack may possibly be used to find the key.

3. **Chosen plaintext** Encrypt *abcdefghijklmnopqrstuvwxyz*

4. **Chosen ciphertext** Decrypt *ABCDEFGHIJKLMNOPQRSTUVWXYZ*

2.4 Vigenère Cipher

The Vigenére Cipher is a variation of the Caesar cipher.

1. **key**: A vector $k = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ of length n with entries from $\mathbb{Z}/26\mathbb{Z}$.

   The key corresponds to a word that is easily remembered.

2. **encryption**: $x \mapsto (x + \alpha_{i \mod n}) \mod 26$

   Thus, in a Vigenère cipher, the ith letter in plaintext gets shifted by α_i where i is taken modulo n. Thus, every nth letter gets shifted by the same amount. So for every nth letter starting at position i, the Vigenère cipher is a Caesar cipher with key α_i.

3. **decrypting**: $y \mapsto (y - \alpha_{i \mod n}) \mod 26$

Example 2.9 Encrypt the phrase "It was the best of times" using a Vigenère cipher with key corresponding to the word "vector"

Solution.

The string to be sent is

$$itwasthebestoftimes$$

The key is $k = (21, 4, 2, 19, 14, 17)$, and the length of k is $n = 6$.

The letters map as follows.

$$\begin{gathered}
i \leftrightarrow 8 \mapsto 8 + \alpha_1 = 8 + 21 \equiv 3 \mod 26 \leftrightarrow D \\
t \leftrightarrow 19 \mapsto 19 + \alpha_2 = 19 + 4 \equiv 23 \mod 26 \leftrightarrow X \\
w \leftrightarrow 22 \mapsto 22 + \alpha_3 = 22 + 2 \equiv 24 \mod 26 \leftrightarrow Y \\
\vdots \\
t \leftrightarrow 19 \mapsto 19 + \alpha_6 = 19 + 17 \equiv 10 \mod 26 \leftrightarrow K \\
h \leftrightarrow 7 \mapsto 7 + \alpha_1 = 7 + 21 \equiv 2 \mod 26 \leftrightarrow C \\
e \leftrightarrow 4 \mapsto 4 + \alpha_2 = 4 + 4 \equiv 8 \mod 26 \leftrightarrow I \\
\vdots
\end{gathered}$$

The results of the encryption are summarized in the following table,

(p.t.)	i	t	w	a	s	t	h	e	b	e	s	t	o	f	t	i	m	e	s
(num)	8	19	22	0	18	19	7	4	1	5	18	19	14	5	19	8	12	5	18
(key)	21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19	14	17	21
(sum)	3	23	24	19	6	10	2	8	3	24	6	10	9	9	21	1	0	22	13
(c.t.)	D	X	Y	T	G	K	C	I	D	Y	G	K	J	J	V	B	A	W	N

So the ciphertext is

$$DXYTGKCIDYGKJJVBAWN$$

Note that the same letter in the plaintext maps to different letters in the ciphertext, depending on position. For example, the first $t \mapsto X$, while the second $t \mapsto K$.

Likewise, the same letter in the ciphertext can represent different letters form the plaintext. For example, $o \mapsto J$ and $f \mapsto J$.

□

Example 2.10 Decrypt the (first few letters) of the ciphertext from the last example.

Solution.

$k = (21, 4, 2, 19, 14, 17)$

$$D \leftrightarrow 3 \mapsto 3 - \alpha_1 = 3 - 21 \equiv 8 \mod 26 \leftrightarrow i$$
$$X \leftrightarrow 23 \mapsto 23 - \alpha_2 = 23 - 4 \equiv 19 \mod 26 \leftrightarrow t$$
$$Y \leftrightarrow 24 \mapsto 24 - \alpha_3 = 24 - 2 \equiv 22 \mod 26 \leftrightarrow w$$

□

2.4.1 Attacks on Vigenère Ciphers

(The different types of attacks are presented in different order, since three of the types of attack are fairly straightforward)

1. **Known plaintext** If the plaintext (along with the ciphertext, as usual) is known, then the key can be obtained by subtracting the plaintext from the ciphertext.

2. **Chosen plaintext** Encrypt the plaintext *aaaaaaa....* The resulting ciphertext will be the key.

3. **Chosen ciphertext** Decrypt the ciphertext *AAAAAAAA....* The resulting plaintext will be the negative of the key.

4. **Ciphertext only attack** If the key length is known, then an attack can be mounted based on frequency analysis. Say the key length is n. If we only consider every nth letter, then the Vigenère cipher on these letters reduces to a shift cipher and frequency analysis can be used to determine the key, since a shift cipher is a special case of substitution cipher.

   Thus, we find the key length. There are two methods.

   - **Method 1**: Compare the ciphertext $\beta_1\beta_2\beta_3\ldots$ with itself displaced by l positions.

     $$\begin{array}{cccccc} \beta_1 & \beta_2 & \beta_3 & \beta_4 & \ldots & \beta_{n-l} \\ \beta_{l+1} & \beta_{l+2} & \beta_{l+3} & \beta_{l+4} & \ldots & \beta_n \end{array}$$

     for each l. Then we record the number $R(l)$ of times times the letter in the top row and the bottom row are the same. That is $R(l) = |\{j|\beta_j = \beta_{j+l}\}|$. If there is a spike in the value of $R(l)$ for a certain value of l, say $l = l_0$, then l_0 is the key length.

     Example 2.11 In the example on the handout, there is a spike at a displacement of 5, so the key length is (probably) 5.

- **Method 2** Search for repetitions of blocks in the ciphertext. I.e. search for occurrences
$$\beta_{j+1}\beta_{j+2}\dots\beta_{j+i} = \beta_{k+1}\beta_{k+2}\dots\beta_{k+i}$$
and compute $|k-j|$.
The differences should match the key length.
Treat repetitions with i large more significantly.

Why these methods work

Consider a vector with English letter frequencies

$$A_0 = (0.082, 0.015, 0.028, \dots, 0.020, 0.001)$$

Define A_i to be A_0 rotated to the right by i positions. That is, entry j of A_i is entry $j-i \mod 26$ of A_0. For example,

$$A_2 = (0.020, 0.001, 0.082, 0.015, \dots)$$

When the plaintext is shifted by i to obtain the cipher text, then the probability that a given letter will appear in the ciphertext is given by the corresponding entry of A_i. For example, if the plaintext is shifted by 2, then A appears in the ciphertext with probability 0.020 and B appears with probability 0.001 since the corresponding entries of A_2 are 0.020 and 0.001.

The dot product $A_0 \cdot A_0 = (0.082)^2+(0.015)^2+(0.028)^2+\dots+(0.020)^2+(0.001)^2 = 0.066$

In fact, $A_i \cdot A_i = 0.066$ for any i. In general the dot products $A_i \cdot A_j$ are given in the following table,

$A_i \cdot A_j$	0.066	0.039	0.032	0.034	0.044	0.033	0.036
$\lvert i-j\rvert$	0	1	2	3	4	5	6

0.039	0.034	0.034	0.037	0.045	0.039	0.043
7	8	9	10	11	12	13

We stop at 13, since the numbers begin to repeat past 13. Note that $A_i \cdot A_j$ is maximized when $|i-j| = 0$ and that the maximum value (0.066) is considerably larger than the second largest value (0.044). (It's not too surprising that it is the largest. Recall that $A_i \cdot A_j = \|A_i\|\|A_j\| \cos\theta$. But $\|A_i\| = \|A_j\|$, so $\|A_i\|\|A_j\| = \|A_i\|^2$, and thus $A_i \cdot A_j = \|A_i\|^2 \cos\theta$. Also, since $A_i > 0$, $\cos\theta < 1$ unless A_i and A_j are parallel. But A_i and A_j are parallel if and only if $i = j$ (in which case, the vectors are equal). Thus $A_i \cdot A_j < A_i \cdot A_i$).

Now, each letter β_k in the top row of ciphertext corresponds to some English letter shifted by $i = \alpha_{k \mod n}$. The probability that $\beta_k = A$ is the first entry of A_i, $(A_i)_1$. The probability that $\beta_k = B$ is $(A_i)_2$, and so forth.

Similarly, the letter β_{k+l}, which appears below β_k in the bottom row of displaced ciphertext, corresponds to some letter of English shifted by $j = \alpha_{k+l \mod n}$. The

probability that $\beta_{k+l} = A$ is $(A_j)_1$. The probability that $\beta_{k+l} = B$ is $(A_j)_2$, and so forth.

Thus, the probability that they are both A is $(A_i)_1(A_j)_1$, the probability that they are both B is $(A_i)_2(A_j)_2$, and so on.

Therefore, the probability that the two letters are the same is the sum of these probabilities over all letters of the alphabet, $(A_i)_1(A_j)_1+(A_i)_2(A_j)_2+\cdots+(A_i)_{26}(A_j)_{26} = A_i \cdot A_j$.

When $i \neq j$, $A_i \cdot A_j \approx 0.038$, but when $i = j$, $A_i \cdot A_j = A_i \cdot A_i = 0.066$. However, if $i = j$, then the letters lying one above the other have been shifted by the same amount, and this happens when the bottom copy of the ciphertext is displaced by an amount equal to the key length (or a multiple of it). Thus, we expect more coincidences when the displacement is equal to (a multiple of) the key length.

For example, the sample ciphertext given on the handout has 326 characters, so we expect $0.066 \times 326 = 21.5$ coincidences when the displacement is equal to the key length, whereas we expect $0.38 \times 326 = 12.4$ coincidences when it is not. These numbers are comparable to the number of coincidences for the various displacements of the sample ciphertext.

2.5 Playfair Cipher (A diagram substitution)

1. **key** To construct the key, first choose a keyword. Deleting 2nd, 3rd, etc. occurrences of letters in the word. The resulting string of letters should have no repeats (and the order of the letters in the string is the same as in the original word). Fill in a 5×5 square with the letters of the string, the square starting with the first square in the top row, and moving right, then down, followed by the remaining letters of the alphabet, and putting i and j in the same square. For example if we choose the word "Playfair", we delete the 2nd "a" to get the string "Playfir". The first row is $PLAYF$, the seconds begin with IR and continues with BCD, etc. The resulting square is

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

2. **Encryption**: Divide the text into pairs of letters. Insert an x between repeated letters. Add an x to complete the last block if necessary.

   - If two letters are not in the same row or column, replace each letter by the letter that is in its row and is in the column of the other letter
   - If two letters are in the same row, replace each letter with the letter immediately to its right (wrapping around if necessary)
   - If two letters are in the same column, replace each letter with the letter immediately below it (wrapping around if necessary)

3. **Decryption**: Reverse the procedure

Example 2.12 Use the above Playfair cipher to encrypt "attack by sea at night"

Solution. First, divide the text into pairs of letters

at ta ck by se ax at ni gh tx

In the row of a and the column of t of the key, there is an F, and in the row of t and the column of a, there is a Q, so

$$at \mapsto FQ$$

In the row of t, and column of a, there is a Q, and in the row of a and column of t there is an F, so

$$ta \mapsto QF$$

All blocks up to ni can be encrypted similarly, since the letters in each of these blocks do not appear in the same row or column. Since n and i are in the same column of the key and the letters U and E lie below the letters n and i respectively,

$$ni \mapsto UE$$

Since g and h are in the same row, and the letters H and K lie to the right of g and h respectively,

$$gh \mapsto HK$$

So the ciphertext is

FQ QF KS CA NK YW FQ UE HK SZ

(The encrypted message is, of course, sent without the spaces.) □

Example 2.13 Decrypt the ciphertext from the preceding example.

Solution. In the row of F and the column of Q, there is an a, and in the row of Q and column of F, there is a t, so $FQ \mapsto at$

Both U and E are in the same column. The letters above U and E in the key are n and i, so $UE \mapsto ni$.

Both H and K are in the same row. The letters preceding H and K are g and h, so $HK \mapsto gh$. □

2.5.1 Attacks on Playfair

1. **Ciphertext only attack**:
   - Digram frequencies are known.
     - The most common digrams are *th*, *he an in*, *re*, *es*, etc. Common digrams in the ciphertext should correspond to common digrams in the plaintext.
     - Note that *er* and *re* are both common. If TB and BT are common in the ciphertext, it is probable that B, T, E, R are the corners of a rectangle.
   - Last row is predictable, unless keyword is long.
   - Each plaintext letter has only 5 ciphertext equivalents.
2. **Known plaintext**: Reconstruct blocks from pairs of letters. For example, if $ab \to CD$ then we have either

a	...	C
	⋮	
D	...	b

,

a	C	...	b	D

or

a
C
⋯
b
D

   If $ab \mapsto BC$ then either

a	b/B	C

or

a
b/B
C

   If $ab \mapsto CA$ then

b	a/A	C

or

b
a/A
C

3. **Chosen plaintext**: Encrypt various (judiciously chosen) letter pairs to fill in the table. (Using techniques similar to those from pt. 2)
4. **Chosen ciphertext**: Decrypt various (judiciously chosen) letter pairs to fill in the table.

2.6 ADFXG Cipher

As in the Playfair cipher, we put the letters into a 5×5 matrix with i and j in the same entry, where the rows and columns are indexed by the letters $ADFXG$, in that order. For example

	A	D	F	G	X
A	p	g	c	e	n
D	b	q	o	z	r
F	s	l	a	f	t
G	m	d	v	i	w
X	k	u	y	x	h

Each plaintext letter is replaced by the label of its row and column. For example, $s \mapsto FA$ because s is in row F and column A, and $z \mapsto DG$ since z is in row D and column G. Each letter maps to a pair of letters If they plaintext is "Kaiser Wilhelm", then the text (not ciphertext) is

XA FF GG FA AG DX GX GG FD XX AG GD GA

Note that, a this stage, this is just a substitution cipher in disguise. Each letter has been mapped to a pair of letters. The next step increases the complexity significantly. Choose a keyword, *Rhein* for example, and put the ciphertext into the matrix whose columns are labelled by the keyword:

R	H	E	I	N
X	A	F	F	G
G	F	A	A	G
D	X	G	X	G
G	F	D	X	X
A	G	F	D	G
A				

Now, reorder the columns so that the labels are in alphabetical order

E	H	I	N	R
F	A	F	G	X
A	F	A	G	G
G	X	X	G	D
D	F	X	X	G
F	G	D	G	A
				A

The ciphertext is obtained by reading down the columns in order (not including the labels):

$$FAGDFAGXFGFAXXDGGGXGXGDGAA$$

Decryption: From the length of the keyword, and the length of the ciphertext, the length of each column is determined. If the key length is k and the length of the ciphertext is m,

then number of "long" is the remainder from dividing m by k. The long columns go with the first letters of the keyword, and the short columns go with the last word.

The letters are placed into columns, which are reordered to match the keyword. The matrix can be used to recover the plaintext.

2.6.1 Attacks

We will only do a ciphertext only attack. Suppose that two messages begin with the same text, and the same key is used for both. For example "Kaiser Wilhelm..." and "Kaiser will leave..." Then we get

R	H	E	I	N
X	A	F	F	G
G	F	A	A	G
D	X	G	X	G
G	F	D	X	X
A	G	F	D	G
A				

R	H	E	I	N
X	A	F	F	G
G	F	A	A	G
D	X	G	X	G
G	F	D	F	D
F	D	A	G	F
F	G	F	A	G

which then becomes

E	H	I	N	R
F	A	F	G	X
A	F	A	G	G
G	X	X	G	D
D	F	X	X	G
F	G	D	G	A
				A

E	H	I	N	R
F	A	F	G	X
A	F	A	G	G
G	X	X	G	D
D	F	F	D	G
A	D	G	F	F
F	G	A	G	F
.	.	.	.	.

Thus, the ciphertexts for both are

FAGDF...	AFXFG ...	FAXXD...	GGGXG...	XGDGAA...
FAGDAF...	AFXFDG...	FAXFGA...	GGGDFG...	XGDGFF...

When the two plaintexts begin with the same texts, the beginning of each column also starts with the same text, and these yield blocks of ciphertext that start with the same letters. Therefore, blocks of that are the same in both ciphertexts (may) correspond to columns that are the same. The number of blocks is the key length. So we look for blocks of ciphertext that start with the same letters.

Once the beginning of blocks are determined, each ciphertext is divided into short and long blocks. If block i is long in both texts, they go to the left, if block i is short in both texts,

they go on the right. If block i is short in one text, but long in the other, they go in the middle.

Frequency analysis can be used to determine how to order the the different columns. For example, $e \mapsto AG$, causing AG to appear frequently after the first step. For each ordering, look for frequently occurring pairs.

The letters $ADFGX$ were chosen because their Morse code equivalents are not easily confused. Later, an $ADFGVX$ cipher was used, which allowed for the use of numbers and all 26 letters.

Chapter 3

Mathematical Tools

3.1 Divisibility

Definition 3.1 Let $a, b \in \mathbb{Z}$, $a \neq 0$. We say that a *divides* b and write $a|b$ if there is some number $x \in \mathbb{Z}$ such that $b = ax$.

In other words, $b/a \in \mathbb{Z}$. Instead of saying "a divides b", we can also say b is divisible by a, or a is a divisor of b.

Definition 3.2 If $a|b$ and $0 < a < b$, then a is a *proper* divisor of b.

Note:

1. $a|0$ for all $a \in Z$
2. $0|b$ does not make sense

The following theorem summarizes some useful properties of divisibility.

Theorem 3.1 *1. If $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$.*

2. If $a|b$ and $b|c$, then $a|c$.

3. If $a|b$ and $a|c$, then $a|(bx + cy)$ for all $x, y \in \mathbb{Z}$.

4. If $a|b$ and $b|a$, then $a = \pm b$.

5. If $a|b$ and $a > 0$, $b > 0$, then $a \leq b$.

6. *If $a|b$, then $qa|qb$ for all $q \in \mathbb{Z}$, $q \neq 0$,*

Proof.

1. Since $b = ma$ we have $bc = mac$.
2. Since $b = ma$ and $c = nb$ we have $c = nb = n(ma)$.
3. Since $b = ma$ and $c = na$ we have $bx + cy = max + nay = a(mx + ny)$.
4. Since $b = ma$, $a = nb$ we see that $a = nma$. Thus $nm = 1$ and so either $n = m = 1$ or $n = m = -1$.
5. Since $b = ma$, $m = b/a \in \mathbb{Z}$. Since both a and b are positive, so is m. Hence m is a positive integer and so $m \geq 1$. Thus $ma \geq a$ and thus $b \geq a$.
6. Since $b = na$ we have $qb = nqa = (nq)a$.

□

Theorem 3.2 *(Division Algorithm) Let $a, b \in \mathbb{Z}$ with $a \geq 0$. Then there are unique integrs $q, r \in \mathbb{Z}$ such that $b = qa + r$ and $0 \leq r < a$*

The number q is called the *quotient*, r is called the *remainder*, b is called the *dividend*, and a is called the *divisor*.

Note: $r = 0$ if and only if $a|b$

Proof. Consider the sequence

$$\ldots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, \ldots$$

Let r denote the smallest non-negative number in this sequence. Then $0 \leq r < a$ and $r = b - qa$ for some integer q. Therefore, $b = qa + r$.

Now, in order to prove the uniqueness of q and r suppose that $b = q_1a + r_1$ and $b = q_2a + r_2$. We will show that $r_1 = r_2$ and $q_1 = q_2$.

First, we show that $r_1 = r_2$. We proceed by contradiction. So assume that $r_1 \neq r_2$. Then, without loss of generality, $r_1 > r_2$, so $0 \leq r_1 < r_2 < a$. Therefore

$$0 < r_2 - r_1 < a.$$

But $r_1 = b - q_1a$ and $r_2 = b - q_2a$, so $r_2 - r_1 = (-q_2 + q_1)a$ is divisible by a. Therefore $a \leq r_2 - r_1$, a contradiction to $r_2 - r_1 < a$. Thus $r_1 = r_2$. So $b - q_1a = b - q_2a$, and therefore $q_1 = q_2$. □

Note An algorithm exists to find q and r: long division.

Definition 3.3 $a \in \mathbb{Z}$ is a *common divisor* of b and c if $a|b$ and $a|c$.

Note: $b \neq 0 \Rightarrow a \leq |b|$ if $a|b$. Thus, if $b \neq 0$ or $c \neq 0$, then there is a greatest number among $\{a : a|b \quad \text{and} \quad a|c\}$. This is called the *greatest common divisor* of a and b, denoted (a, b) or $\gcd(a, b)$. Similarly we define (a, b, c) (or $\gcd(a, b, c)$) to be the greatest integer dividing a, b and c when at least one of these is non-zero.

Example 3.1

$$\begin{aligned} (-12, -18) &= 6 \\ (4, -5) &= 1 \\ (3, -9, 15) &= 3 \\ (0, b) = |b| & \\ (6, 15, -21) = 3 & \end{aligned}$$

Notes:

1. $(0, 0)$ is not defined.
2. $(a, b) \geq 1$.

Theorem 3.3 *Let $g = (b, c)$. Then there are numbers $x_0, y_0 \in \mathbb{Z}$ such that $g = (b, c) = bx_0 + cy_0$. In fact, g is the smallest positive number of the form $bx + cy$.*

Proof. Let x_0 and y_0 be two integers which give the smallest positive number of the form $bx + cy$. That is, if $bx + cy > 0$, then

$$bx + cy \geq bx_0 + cy_0$$

Let $l = bx_0 + cy_0$ and $S = \{bx + cy | x, y \in \mathbb{Z}, bx + cy > 0\}$. Then $l = \min S$.

Claim: $l|b$.

Proof of claim: By contradiction. Assume that $l|b$. Then $b = ql + r$, where $0 < r < l$. Then $r = b - ql = bq(bx_0 + cy_0) = (1 - qx_0)b + cqy_0$. Thus $r \in S$ and $r < l$ a contradiction.

By a similar argument, $l|c$.

Since g divides both b and c, $b = gB$ and $c = gC$ for some $B, C \in \mathbb{Z}$ and $l = bx_0 + cy_0 = gBx_0 + gCy_0$. Therefore $g|l$, and so $g \leq l$. But $g < l$is impossible, since g is the greatest common divisor. Therefore, $g = l$. □

3.1.1 Euclidean Algorithm

The Euclidean Algorithm makes use of the division algorithm to find the greatest common divisor of two numbers.

If $a, b \in \mathbb{Z}$ where $a \neq 0$, then (a, b) is the last nonzero remainder in the following list of equations obtained from the Division Algorithm.

$$\begin{aligned}
b &= q_1 a + r_1 \quad \text{where} 0 < r_1 < |a| && (3.1)\\
a &= q_2 r_1 + r_2 \quad \text{where} 0 < r_2 < r_1 && (3.2)\\
r_1 &= q_3 r_2 + r_3 \quad \text{where} 0 < r_3 < r_2 && (3.3)\\
&\vdots && (3.4)\\
r_{n-2} &= q_n r_{n-1} + r_n \quad \text{where} 0 < r_n < r_{n-1} && (3.5)\\
r_{n-1} &= q_{n+1} r_n + 0 && (3.6)
\end{aligned}$$

Example 3.2 Find the greatest common divisor of 42823 and 6409.

Solution.

$$\begin{aligned}
42823 &= 6(6409) + \underbrace{4369}_{=r_1}\\
6409 &= (4369) + \underbrace{2040}_{=r_2}\\
4369 &= 2(2040) + \underbrace{289}_{=r_3}\\
2040 &= 7(289) + \underbrace{17}_{=r_4}\\
289 &= 17(\underline{17}) + 0
\end{aligned}$$

□

Example 3.3 Find x and y such that

$$42823x + 6409y = 17$$

Solution. We use the find x_i and y_i such that

$$42823x + 6409y = r_i$$

and then use $x = x_4$ and $y = y_4$. Set $r_0 = 6409$ and $r_{-1} = 42823$. Then

$$\begin{aligned} x_i(42823) + y_i(6409) &= r_i = 42823 \\ 1(42823) + 0(6409) &= r_{-1} = 42823 \\ 0(42823) + 1(6409) &= r_0 = 6409 \\ 1(42823) - 6(6409) &= r_1 = 4369 \end{aligned}$$

So

$$\begin{aligned} r_2 = 2040 &= 6409 - 1(4369) \\ &= 6409 - 1[1(42823) - 6(6409)] \\ &= -1(42823) + 7(6409) \end{aligned}$$

So $x_2 = -1$ and $y_2 = 7$. Then

$$\begin{aligned} r_3 = 289 &= 4369 - 2(2040) \\ &= [1(42823) - 6(6409)] - 2[-1(42823) + 7(6409)] \\ &= 3(42823) - 20(6409) \end{aligned}$$

So $x_3 = 3$, and $y_3 = -20$. Finally,

$$\begin{aligned} r_4 = 17 &= 2040 - 7(289) \\ &= [-1(42823) + 7(6409)] - 7[3(42823) - 20(6409)] \\ &= -22(42823) + 147(6409) \end{aligned}$$

Note: There are other solutions (x, y) to

$$4283x + 6409y = 17$$

□

Theorem 3.4 *Let $b_1, \ldots, b_n$ be integers, not all zero. Let $g = (b_1, \ldots, b_n)$. Then there are integers $x_1, \ldots, x_n$ such that*

$$g = b_1x_1 + b_2x_2 + \cdots + b_nx_n$$

Furthermore, g is the least integer in the set

$$S = \{b_1x_2 + \cdots + b_nx_n | x_1, \ldots, x_n \in \mathbb{Z}, b_1x_1 + \cdots + b_n > 0\}$$

Proof. Similar to the preceding theorem. □

Theorem 3.5 *Let $m > 0, m \in \mathbb{Z}$. Then $(ma, mb) = m(a, b)$.*

Proof. (ma, mb) is the least positive value of $max + mby$. $max + mby = m(ax + by)$ is m times the least positive value of $ax+by$. m times the least positive value of $ax+by$ is $m(a, b)$. □

Theorem 3.6 *1. If $d|a$ and $d|b$ and $d > 0$, then $(a/d, b/d) = \frac{1}{d}(a, b)$*

2. If $g = (a, b)$ then $(a/g, b/g) = 1$

Proof.

1. Same as preceding proof, using $m = 1/d$
2. Take $d = g$ in 1.: $(a/g, b/g) = \frac{1}{g}(a, b) = \frac{1}{g}g = 1$

□

Theorem 3.7 *If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$.*

Proof. Write $1 = ax_0 + my_0$ and $1 = bx_1 + my_1$. Then

$$\begin{aligned}(ax_0)(bx_1) &= (1 - my_0)(1 - my_1)\\ &= 1 - m(y_0 + y_1 - my_0y_1)\end{aligned}$$

Therefore, $1 = ab(x_0x_1) + m(y_0 + y_1 - my_0y_1)$, so $(ab, m) = 1$. □

Definition 3.4 We say that a and b are *relatively prime* if $(a, b) = 1$ and that $a_1, \ldots, a_n$ are *relatively prime* if $(a_1, \ldots, a_n) = 1$. We say that $a_1, \ldots, a_n$ are *pairwise prime* if $(a_i, a_j) = 1$ for all $i \neq j$.

Theorem 3.8 *If $c|ab$ and $(b, c) = 1$, then $c|a$.*

Proof. By Theorem 3.5 $(ab, ac) = a(b, c) = a \cdot 1 = a$. Now, $c|ab$ and $c|ac$, so $c|(ab, ac) = a$. □

Theorem 3.9

$$\begin{aligned}(a,b) &= (b,a) = (-a,b)\\ (a,b) &= (a,b+ax) \quad \textit{for all } x \in \mathbb{Z}\end{aligned}$$

Definition 3.5 Let $a_1, \ldots, a_k$ be integers different from 0. Then b is a common multiple of $a_1, \ldots, a_k$ if each $a_i|b$. The smallest positive common multiple is the *least common multiple (lcm)* which is denote $[a_1, \ldots, a_k]$.

Theorem 3.10 *If b is any common multiple of $a_1, \ldots, a_k$, then $[a_1, \ldots, a_k]|b$. In other words, if $h = [a_1, \ldots, a_k]$, then the only common multiples of $a_1, \ldots, a_k$ are $0, \pm h, \pm 2h, \pm 3h$.*

Proof. Let m be any common multiple. Divide m by h: $m = qh + r, 0 \leq r < h$.

We need to show that $r = 0$. Assume $r \neq 0$. Then $a_i|m$ and $a_i|h$, so $a_i|r$. Therefore, r is a positive common multiple of $a_1, \ldots, a_k$. But $r < h$, a contradiction. □

Theorem 3.11 *Let a, b be non-zero and $m > 0$. Then $[ma, mb] = m[a, b]$. Also, $[a, b] \cdot (a, b) = |ab|$.*

Proof. Let $H = [ma, mb]$ and $h = [a, b]$. Then mh is a multiple of ma and mb. Therefore, $H \leq mh$. Also, H is a multiple of ma and mb, so H/m is a multiple of a and b, so $H/m \geq h$. Therefore, $H \geq mh$.

Also, $WLOG$, $a > 0, b > 0$. First, consider $(a, b) = 1$. Then $[a, b] = ma$ for some m. Now $b|ma$ and $(a, b) = 1$, so $b|m$. Therefore $b \leq m$ and $ba \leq ma$. But ba is a common multiple of a, b, so $ba \leq ma = [a, b]$. Therefore, $[a, b] = ab$.

Now consider $(a, b) = g > 1$. Then $(a/g, b/g) = 1$, so $(a/g, b/g)[a/g, b/g] = \frac{a}{g}\frac{b}{g}$. Therefore, $g(a/g, b/g) \cdot g[a/g, b/g] = ab$ i.e. $(a, b)[a, b] = ab$. □

Definition 3.6 An integer $p > 1$ is *prime* if the only positive divisors of p are 1 and p.

Definition 3.7 If an integer $a > 1$ is not prime, then it is said to be *composite*.

Note: 0 and 1 and all negative numbers are neither prime nor composite.

Example 3.4 2,3,5,7,11, 17 are all prime.

4,6,8,9,10 are composite.

Theorem 3.12 *(Fundamental Theorem of Arithmetic) Every integer greater than 1 can be expressed as a product of primes. Furthermore, this expression is unique except for the order of the factors.*

Example 3.5 (non-example). Let E be the set of all even numbers. Then $2, 6, 10, 30$ are "prime" in E. That is, there are no divisors of these numbers in E, other than 1 and themselves. $60 = 2(30)$ and $60 = 6(10)$, and $36 = 6(6) = 2(18)$. In both cases, there are two distinct factorizations of the numbers into primes in E.

Example 3.6 (non-example) Let $F = \mathbb{Q}[\sqrt{-6}] = \{a + b\sqrt{-6} | a, b \in \mathbb{Q}\}$. $10 = (2)(5)$ and $10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$

Before we prove the FTA, we prove the following theorem

Theorem 3.13 *Let p be a prime. If $p|ab$, then $p|a$ or $p|b$. More generally, if $p|a_1 \dots a_n$ then $p|a_i$ for some i.*

Proof. We proceed by induction on n. First consider the case $n = 2$. Suppose that $p|a_1a_2$. If $p \not| a_1$, then $(a_1, p) = 1$ and so, by a previous theorem, $p|a_2$. Therefore, $p|a_1$ or $p|a_2$.

Now we assume that the theorem is true for $n-1$ and show that it holds for n. So we make the following induction hypothesis: If $p|a_1 \cdots a_{n-1}$ means then $p|a_1$ or $p|a_2$ or $\cdots$ or $p|a_{n-1}$. Suppose further that $p|a_1a_2 \dots a_n$. If $p \not| a_n$, then $(p, a_n) = 1$. Since $p|(a_1 \cdots a_n)a_n$ but $p \not| a_n$, we must have $p|a_1a_2 \cdots a_{n-1}$. Therefore, by the induction hypothesis, $p|a_1$ or $p|a_2$ or $\cdots$ or $p|a_{n-1}$, and therefore, $p|a_1$ or $p|a_2$ or $\cdots$ or $p|a_n$ □

Proof.(Proof of the fundamental Theorem of Arithmetic) We proceed by contradiction. So suppose the theorem is false. Then there is a number N with two different factorizations $N = p_1 \cdots p_r = q_1 \cdots q_s$. If any prime occurs on both sides of the equation, we may cancel it from both sides to get a number $M = p_1 \cdots p_m = q_1 \cdots q_n$ where $p_1 \notin \{q_1, \cdots, q_n\}$. But $p_1|M = q_1 \cdots q_n$. Thus, there is a number i such that $p_1|q_i$. But q_1 is a prime, so $p_1 = q_i$, contradicting distinct prime factors. □

Theorem 3.14 *(Due to Euclid) There is an infinite number of primes*

Proof. Suppose not. Then there are only r primes, $p_1 = 2, p_2 = 3$ $p_3 = 5 \dots p_r$. Define $n = p_1p_2 \cdots p_r + 1$. Then $p_1 \not| n, p_2 \not| n, \dots p_r \not| n$, because division by p_i produces a remainder of 1 for all i. But n is either prime or has a prime factor other than $p_1, \dots, p_r$. Thus, there are more than r primes, and so there cannot be finitely many primes. □

Note: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \cdot 13 + 1 = 59 \cdot 509$

Theorem 3.15 *There are arbitrarily large gaps in the sequence of primes. I.e. for any $k \in \mathbb{N}$, there is a sequence of k composite integers.*

Proof. Consider the sequence $(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+(k+1)$. We have $j|(k+1)!+j$ for each j from 2 to $k+1$. Hence each of the numbers in the sequence is composite. □

3.2 Binomial Theorem

Let $n, k \in N$. Then we define

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Theorem 3.16 *If S is a set of n different objects, then there are exactly $\binom{n}{k}$ subsets of S of size k.*

Proof. Let $S = \{1, 2, \ldots, n\}$. There are $n!$ permutations of S (ordered sequences) $\sigma_1\sigma_2\cdots\sigma_n$:

n choices for σ_1

$n-1$ choices for σ_2

$\vdots$

1 choice for σ_n

Now pick a subset $A \subseteq S$ with $|A| = k$. We get a permutation of S via a permutation $a_1, a_2, \ldots a_k$ of A followed by a permutation $b_1, \ldots, b_{n-k}$ of $S \setminus A$: $a_1, \ldots, a_k, b1, \ldots, b_{n-k}$.

Now, using A, we get $k!(n-k)!$ of the permutation of S this way. Doing this for all sets $A_1, \ldots, A_x$ of size k we get $xk!(n-k)! = n!$, so $x = n!/(k!(n-k)!)$. □

Theorem 3.17 *The product of k consecutive integers is divisible by $k!$*

*Proof.*Let $m = n(n-1)(n-2) = (n-k)\cdots(n-k+1)$.

- If $n \geq k$, then $\frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{m}{k!}$ Therefore, $m = k!\binom{n}{k}$ and m is divisible by $k!$.
- If $0 \leq n \leq k$, then $m = 0$.

- If $n < 0$, then

$$\begin{aligned} m &= n(n-1)\cdots(n-k+1) \\ &= (-n)(-n+1)\cdots(-n+k-1)(-1)^k \\ &= (-1)^k\binom{-n+k-1}{k}k! \quad \text{where } -n+k-1 \geq k \end{aligned}$$

Therefore, $\frac{m}{k!} = (-1)^k\binom{-n+k-1}{k} \in \mathbb{Z}$ by the previous theorem.

□

Note: $\binom{n}{k} = \binom{n}{n-k}$.

Theorem 3.18 *(Binomial Theorem)*

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$$

3.3 Congruences

Let $m \in \mathbb{Z}$, $m \neq 0$. If m divides $a-b$, then we say that a is congruent to b modulo m and we write $a \equiv b(\mod m)$. Otherwise we write $a \not\equiv b \mod m$. Sometimes we write $a \equiv b(m)$ instead of $a \equiv b \mod m$, or just $\equiv$ with (m) or $\mod m$ understood.

Example 3.7

1. $12 \equiv 32 \mod 10$
2. $12 \not\equiv 32 \mod 7$
3. $29 \equiv -1 \mod 3$
4. $-28 \equiv 0 \mod 14$

Note: Since $a \equiv b \mod m$ if and only if $a \equiv b \mod -m$, we usually work only with positive moduli.

Theorem 3.19 *Let $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}$, $m \neq 0$. Then*

1. *$a \equiv b \mod m$ if and only if $b \equiv a \mod m$ if and only if $b - a \equiv 0 \mod m$*
2. *If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$*
3. *If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$*
4. *If $a \equiv b \mod m$ and $c \equiv d \mod m$ then $ac = bd \mod m$*

5. *If* $a \equiv b \mod m$ *and* $d|m$, *then* $a \equiv b \mod d$.

6. *If* $a \equiv b \mod m$ *then* $ac \equiv bc \mod mc$.

Proof.

1. $a \equiv b \pmod m$ if and only if $m|(b-a)$ if and only if $m|(a-b)$ if and only if $b \equiv a \pmod m$. Finally $b-a \equiv 0 \pmod m$ if and only if $m|(b-a)-0$ if and only if $m|b-a$.

2. Suppose $a \equiv b \pmod m$ and $b \equiv c \pmod m$. Thus $m|(b-a)$ and $m|(c-b)$. Therefore $m|(c-b)+(b-a) = c-a$. Therefore $a \equiv c \pmod m$.

3. Suppose $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Thus m divides both $b-a$ and $d-c$. Therefore m divides $(b-a)+(d-c) = (b+d)-(a+b)$. Thus $a+c \equiv b+d \pmod m$.

4. Suppose $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then there exists $q_1, q_2 \in \mathbb{Z}$ with $b-a = q_1 m$ and $d-c = q_2 m$. Therefore $bd = (q_1 m + a)(q_2 m + c) = q_1 q_2 m^2 + a q_2 m + c q_1 m + ac = (q_1 q_2 m + a q_2 + c q_1)m + ac$. Thus $m|(bd-ac)$ and so $ac = bd \pmod m$.

5. Suppose $a \equiv b \pmod m$ and $d|m$. Then $m|(b-a)$ and so $d|(b-a)$. Therefore $a \equiv b \pmod d$.

6. Suppose $a \equiv b \pmod m$. Thus $b-a = qm$ for some integer q. Therefore $bc-ac = qmc$ so $mc|(bc-ac)$, i.e., $ac \equiv bc \pmod{mc}$.

□

Theorem 3.20 *Let* f *be a polynomial with integral coefficients. If* $a \equiv b \mod m$ *then* $f(a) \equiv f(b) \mod m$.

Proof. Let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots c_n x^n$

Since $a \equiv b \mod m$, we have $a^2 \equiv b^2 \mod m, \ldots, a^n \equiv b^n \mod m$ (follows from part 4 of previous theorem). Therefore, $c \equiv c_0(m), c_1 a \equiv c_1 b(m), c_2 a^2 \equiv c^2 b^2 \mod (m), \ldots, c_n a^n \equiv c_n b^n(m)$ (also follows from part 4 of previous theorem)

Therefore, $\underbrace{c_0 + c_1 a + \cdots + c_n a^n}_{f(a)} \equiv \underbrace{c_0 + c_1 a + \cdots c_n b^n}_{f(b)} \mod n$ □

Note: If $ax = ay$ and $a \neq 0$, then $x = y$ when $a, x, y \in \mathbb{R}$. However, if $ax \equiv ay$ and $a \not\equiv 0$, it is not always true that $x \equiv y$. For example, If $a = 10, x = 2, y = 23$, and $m = 42$, then $ax = 20$ and $ay = 230 = 20 \mod 42$, so $ax \equiv ay \mod 42$, but $a = 10 \not\equiv b = 23 \mod 42$.

Theorem 3.21 *1.* $ax \equiv ay \mod m$ *if and only if* $x \equiv y \left(\mod \frac{m}{(a,m)} \right)$

2. If $ax \equiv ay(\mod m)$ *and* $(a, m,) = 1$*, then* $x \equiv y$

3.
$$\begin{array}{rcl} x & \equiv & y \mod m_1 \\ x & \equiv & y \mod m_2 \\ & \vdots & \\ x & \equiv & y \mod m_r \end{array} \quad \text{if and only if } x \equiv y \mod [m_1, m_2, \cdots, m_r]$$

Proof.

1. If $ax \equiv ay \mod m$ then $ay - ay = mz$ for some $z \in \mathbb{Z}$. Therefore
$$\frac{a}{(a,m)}(x - y) = \frac{m}{(a,m)}z$$
So
$$\frac{m}{(a,m)} | \frac{a}{(a,m)}$$
But
$$\left(\frac{m}{(a,m)}, \frac{a}{(a,m)} \right) = \frac{1}{(a,m)}(a, m) = 1$$
Thus, $\frac{m}{(a,m)} | (x - y)$ i.e. $x \equiv \left(\mod \frac{m}{(a,m)} \right)$ Conversely, if $x \equiv y \left(\mod \frac{m}{(a,m)} \right)$, then $ax = ay \left(\mod \frac{m}{(a,m)} \right)$. Therefore $ax = ay \mod m$ (sinc $m | \frac{am}{(a,m))}$

2. This is a special case of part 1.

3. $(\Rightarrow) m_i | (x-y)$ for all i. Therefore, $x-y$ is a common multiple of $m_i, \ldots, m_n$. Therefore $[m_1, \ldots, m_r] | (x - y)$. That is, $x = y \mod [m_1, m_2, \ldots, m_r]$
$(\Leftarrow)$ If $x \equiv y \mod [m_1, \ldots, m_r]$, then $x \equiv y(\mod m_i)$ since $m_i | [m_1, m_2, \ldots, m_r]$

□

Definition 3.8 A set of m integers $\{a_1, \ldots, a_m\}$ is a *complete residue system modulo* m if for every integer x, there is a unique i such that $x \equiv a_i \mod m$.

Clearly, there are infinitely many. For example both $\{0, 1, 2, \ldots, m_1\}$ and $\{1, 2, \ldots, m\}$ are complete residue systems module m. Also, both $\{0, 1, 2, 3, 4, 5\}$ and $\{1, 5, 8, 12, 28, -3\}$ complete residue systems modulo 6.

The set $\{x | x \equiv a(\mod m)\}$ for some fixed a is the *congruence class modulo* m *of* a. This is the set of numbers $a, a \pm m, a \pm 2m, a \pm 3m, \ldots$

Theorem 3.22 *If $b \equiv c(\mod m)$, then $(c, m) = (b, m)$.*

Proof. If $b \equiv c \mod m$, then $m|(b - c)$. Therefore, $b - c = mx$ for some $x \in \mathbb{Z}$. Then $b = c + mx$ and so

$$(b, m) = (c + mx, m) = (c, m)$$

□

Definition 3.9 A *reduced residue system modulo m* is a set $\{a_1, \ldots, a_r\}$ such that for all $x \in \mathbb{Z}$ with $(x, m) = 1$, there is a unique i such that $x \equiv a_i \mod m$.

For example, if $m = 6$, then $\{1, 5\}$ is a reduced residue system modulo m. If $m = 15$, then $\{1, 2, 4, 7, 8, 11, 13, 14\}$ is a reduced residue system modulo m

Note: by the previous theorem, we my construct a reduced residue system modulo m by delete from a complete residue system modulo m all a_i such that $(a_i, m) > 1$. Furthermore, every reduced residue system modulo m contains the same number of elements. We denote this number by $\phi(m)$. The function $m \mapsto \phi(m)$ is called the Euler totient function.

Theorem 3.23 *(Fermat's Little Theorem) Let p be prime.*

1. *Then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$*
2. *If $p \not| a$, then $a^{p-1} \equiv 1 \mod p$*

We shall prove the following theorem

Theorem 3.24 *(Euler's Generalization of Fermat's Little Theorem) If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \mod m$*

Proof. Let $\{r_1, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m. Then $\{ar_1, \ldots, ar_{\phi(m)}\}$ is also. Hence for all i there is a unique j such that $r_i \equiv ar_j \mod m$. That is

$$\{r_1, \ldots, r_{\phi(m)}\} = \{ar_1, \ldots, ar_{\phi(m)}\}$$

in some order. Therefore,

$$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} ar_i \mod m$$

Therefore

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} \mod m$$

Now $(r_1, m) \equiv 1$ for all i. Therefore, $(\prod_{i=1}^{\phi(m)}, m) = 1$, and so $a^{\phi(m)} \equiv 1 \mod n$ □

Theorem 3.25 *If $(a, m) = 1$ then there exists an x such that $ax \equiv 1 \mod m$. Furthermore, if $ax_1 \equiv ax_2 \equiv 1$ then $x_1 \equiv x_2 \mod m$. Furthermore, if $ax_1 \equiv ax_2 \equiv 1$ then $x_1 \equiv x_2(m)$. If $(a, m) > 1$, then there is no x such that $ax \equiv 1 \mod m$.*

Proof. If $(a, m) = 1$, then there is some x, y such that $ax + m1 = 1$ ie. $ax = 1 \mod m$. The furthermore is immediate.

Conversely, if $ax = 1$, then $m|ax - 1$, say $ax - 1 = my$. Then $1 = ax - my = ax + m(-y)$. Therefore $1 = (a, m)$. □

Notation: We denote by $\overline{a}$ the residue class such that $a\overline{a} \equiv 1 \mod m$ and reserve a^{-1} for $\frac{1}{a} \in \mathbb{R}$.

Note: $\overline{a} = a^{\phi(m)-1}$

Lemma 3.26 *Let p be a prime. Then $x^2 \equiv 1 \mod p$ if and only if $x \equiv \pm 1 \mod p$*

Proof.

$$\begin{aligned} x^2 \equiv 1 &\Leftrightarrow x^2 - 1 \equiv 0 \mod p \\ &\Leftrightarrow (x-1)(x+1) \equiv 0 \mod p \\ &\Leftrightarrow p|(x-1)(x+1) \\ &\Leftrightarrow p|(x-1) \text{ or } p|(x+1) \\ &\Leftrightarrow x \equiv 1 \mod p \text{ or } x \equiv -1 \mod p \end{aligned}$$

□

Theorem 3.27 *(Wilson's Theorem) If p is a prime then $(p-1)! \equiv -1 \mod p$*

Proof. It is easy to check for $p = 2$ or 3. Therefore, suppose $p \geq 5$. Let $1 \leq a \leq p-1$. Then $(a, p) = 1$ and there is a unique number $\overline{a}$ such that $1 \leq \overline{a} \leq p-1$ and $a\overline{a} = 1$.

Note: $a = \overline{a}$ if and only if $aa = \equiv 1$ if and only if $a \equiv \pm 1 \mod p$. Therefore

$$\prod_{a=2}^{p-2} a \equiv 1 \mod p$$

and so

$$(p-1)! = \prod_{a=1}^{p-1} a = \prod_{a=2}^{p-2} a \cdot 1 \cdot (p-1) \equiv 1 \cdot 1(p-1) \equiv -1 \mod p$$

□

Theorem 3.28 *Let p be a prime. Then $x^2 \equiv -1(p)$ for some x if and only if $p = 2$ or $\equiv 1 \mod 4$.*

Proof. If $p = 2$, then take $x = 1$. Now suppose that p is odd. Then, by Wilson's Theorem,

$$-1 \equiv \left(1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdot \cdots \cdot (p-j) \cdot \cdots \cdot (p-2) \cdot (p-1)\right) \mod p$$

I.e.

$$\begin{aligned} -1 &\equiv \prod_{j=1}^{(p-1)/2} j(p-j) \mod p \\ &\equiv \prod_{j=1}^{(p-1)/2} -j^2(-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} j^2 \mod p \end{aligned}$$

($\Leftarrow$) If $p \equiv 1 \mod 4$, this gives $-1 \equiv \prod_{j=1}^{(p-1)/2} j^2 = \left(\prod_{j=1}^{(p-1)/2} j\right)^2$ and therefore, $x = \prod_{j=1}^{(p-1)/2} j$ is a solution.

($\Rightarrow$) Conversely, assume that $x^2 = -1 \mod p$. Then $p \not| x$, clearly ($p > 2$ still) Therefore,

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \mod p$$

and so

$$x^{p-1} \equiv (-1)^{(p-1)/2} \mod p$$

But, by Fermat's little theorem, $x^{p-1} = 1 \mod p$. Therefore, $(-1)^{(p-1)/2} \equiv 1 \mod p$. If $(-1)^{(p-1)/2} = -1$, this means $p|2$, a contradiction. So $(-1)^{(p-1)/2} = 1$. I.e. $p \equiv 1 \mod 4$. □

Lemma 3.29 *If p is a prime number and $p \equiv 1 \mod 4$, then there are numbers a, b such that $p = a^2 + b^2$.*

Proof. By the previous theorem, there is a number x such that $x^2 \equiv 1 \mod p$.

Define $f(u, v) = u + xv$ and $K = [\sqrt{p}] \in \mathbb{N}$ ($[x]$ is x rounded down to nearest). Then

$$K < \sqrt{p} < K + 1$$

Consider pairs (u, v) such that $0 \leq u \leq K$ and $0 \leq v \leq K$. There are $(k+1)^2$ such pairs. Also, since $(k+1) > \sqrt{p}$, $(K+1)^2 > p$. By the pigeonhole principle, there are two pairs (u_1, v_1) and (u_2, v_2) with $0 \leq u_i, v_i \leq K$, $f(u_1, v_i) \equiv f(u_2, v_2) \mod p$, and $(u_1, v_1) \neq (u_2, v_2)$. I.e. $u_1 + xv_1 \equiv u_2 + xv_2 \mod p$. Define $a = u_1 - u_2, b = v_1 - v_2$ ($(a, b) \neq (0, 0)$). Then $a \equiv -xb$. Therefore, $a^2 \equiv x^2 b^2 > 0$. Also, $0 \leq u_1, u_2 \leq K$. So $a \leq K$ and $-K \leq a$. Similarly, $K \leq b \leq K$. Therefore $a^2 \leq K^2 < p$. and $b^2 \leq K^2 < p$. Therefore, $0 < a^2 + b^2 < 2p$. Since $p|a^2 + b^2$, we must have $p = a^2 + b^2$. □

Theorem 3.30 *Let q be prime and assume $q|a^2+b^2$. If $qq \equiv 3 \mod 4$, then $q|a$ and $q|b$.*

Proof. If $q \not| a$ or $q \not| b$ and $q|a^2+b^2$ then $q \not\equiv 3 \mod 4$.

Assume, without loss of generality, that $q \not| a$ and $q|a^2+b^2$. Since $q \not| a$, we have $(q,a)=1$. Then there is some number $\overline{a}$ such that $a\overline{a} = 1 \mod q$. Multiply $a^2 \equiv -b^2 \mod q$ by $\overline{a}^2$ to get $1 = -\overline{a}^2 b^2 \mod q$. Then $x = \overline{a}b$ is a solution of $x^2 \equiv -1 \mod q$. Therefore $q \equiv 1 \mod 4$ or $q = 2$ and so $q \not\equiv 3 \mod 4$. □

Theorem 3.31 *(Fermat) Factor n into primes as*

$$n = 2^\alpha \prod_{p_i \equiv 1(4)} p_i^{\beta_i} \prod_{q_j \equiv 3(4)} q_j^{\gamma_j}$$

. Then there are numbers a, b such that $n = a^2+b^2$ if and only if each γ_j is even.

Proof. **Note**: $(a^2+b^2)(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$ for all $a,b,c,d \in \mathbb{R}$. Thus, if m and n are both the sum of two squares then so is mn.

Also, $2 = 1^2+1^2$ and if $p \equiv 1 \mod 4$, then p is the sum of 2 squares. Also, if $q^2 = q^2+0^2$. This proves ($\Leftarrow$)

Now, suppose that $n = a^2+b^2, q \equiv 3 \mod 4$, $q \equiv 3 \mod 4$ and $\gamma > 0$. Then by the previous lemma, $q|a$ and $g|b$. Therefore $q^2|n$. I.e. $\gamma \geq 2$. Then

$$\frac{n}{q^2} = \left(\frac{a}{q}\right)^2 + \left(\frac{b}{q}\right)^2$$

Applying the same argument to $\frac{n}{q^2}$, we see that if $\gamma > 2$, then $\gamma \geq 4$. Since this process must terminate, we conclude that γ is even and $q^{\gamma/2}$ divides a and b. □

3.4 Solutions of Congruences

Consider a polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in \mathbb{Z}$. If $u \in Z$ and $f(u) \equiv 0 \mod m$ then we say u is a solution of the congruence

$$f(x) \equiv 0 \mod m$$

This depends on both f and m.

Note: An earlier theorem shows that if $u \equiv v(\mod m)$ then $f(u) \equiv f(v)$. Hence, we will say that $x \equiv u \mod m$ is a solution to $f(x) \equiv 0 \mod m$ if $f(u) \equiv 0 \mod m$.

Example 3.8 $x^2 - 2x + 6 \equiv 0 \mod 14$ has solutions $x \equiv 4$ and $x \equiv 12$.

Example 3.9 $x^2 - 7x + 2 \equiv 0 \mod 10$ has $x \equiv 3, 4, 8, 9$ as (only) solutions.

Definition 3.10 Let $r_1, \ldots, r_m$ denote a complete residue system modulo m. The number of solutions of $f(x) \equiv 0 \mod m$ is the number of r_i such that $f(r_i) \equiv 0 \mod m$

Example 3.10 $x^2 + 1 \equiv 0 \mod 5$ has 2 solutions.

$x^2 + 1 \equiv 0 \mod 7$ has no solutions.

$x^2 - 1 \equiv 0 \mod 8$ has 4 solutions.

Definition 3.11 Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_0$. Let j be the largest integer such that $a \not\equiv 0 \mod m$ (if such a j exists) Then the degree of the congruence $f(x) \equiv 0 \mod m$ is j. If no such j exists, we don't assign a a degree.

For example, each of the polynomials in the last example have degree 2. The degree of the congruence $5x^4 + 2x^3 + 1 \equiv 0 \mod 5$ is 2, since the coefficient of x^4 is congruent to $0 \mod 5$.

3.4.1 Linear Congruences

A congruence of degree 1 is called a *linear congruence*

Theorem 3.32 *Let $a, b \in \mathbb{Z}, m \in \mathbb{N}(m \neq 0)$. Let $g = (a, m)$. The congruence $ax \equiv b \mod m$ has a solution if and only if $g|b$. If $g|b$ then the solutions form an arithmetic sequence with common difference m/g and length g.*

Example 3.11 Consider the congruence $6x \equiv 9 \mod 21$. $g = (6, 21) = 3|9$ so the congruence has a solution. The common difference of the solutions is $21/3 = 7$, and the length of the solution sequence is 3. Since 5 is a solution, the solutions are 5, $5 + 7$, and $5 + 2 \cdot 7 = 19$.

Proof. By the definition of congruence, we want want to determine whether or not there are x and y such that

$$ax + my = b$$

($\Rightarrow$)Since $g = (a, m)$, we know that g divides the LHS. Hence, if $g \not| b$, then no solutions exist.

($\Leftarrow$) Now, suppose that $g|b$. Write $b = g\beta$, $a = g\alpha$, and $m = g\mu$. Thus, we want to determine whether or not there are x and y such that

$$g\alpha x + g\mu y = g\beta$$

That is, such that

$$\alpha x + \mu y = \beta$$

Claim: There is some number $\overline{\alpha}$ such that $\overline{\alpha}\alpha \equiv 1 \mod \mu$.

Proof of Claim Because $(\alpha, \mu) = 1$, there are numbers A and B such that $A\alpha + B\mu = 1$. Therefore $A\alpha \equiv 1 \mod \mu$. Pick $\overline{\alpha} = A$.

Now, multiply by $\overline{\alpha}$ to get $\overline{\alpha}\alpha x + \overline{\alpha}\mu y = \overline{\alpha}\beta$. Then

$$x \equiv \overline{\alpha}\beta \mod \mu.$$

Thus $x = \overline{\alpha}\beta,\ \overline{\alpha}\beta + \mu,\ \overline{\alpha}\beta + 2\mu,\ \ldots, \overline{\alpha}\beta + (g-1)\mu$ are all solutions to $ax \equiv b \mod m$. Note $\overline{\alpha}\beta + g\mu = \overline{\alpha}\beta + m \equiv \alpha\beta \mod m$ □

3.5 Chinese Remainder Theorem

Theorem 3.33 *Suppose $(m, n) = 1$. Given integers a and b, there exists exactly one solution $x \mod mn$ to the simultaneous congruences*

$$x \equiv a \mod m, \qquad x \equiv b \mod n$$

Example 3.12 Solve the system of congruences

$$\begin{aligned} x &\equiv 3 \mod 7 \\ x &\equiv 5 \mod 15 \end{aligned}$$

Solution. Since $(7, 15) = 1$, there exists exactly one solution x between 0 and $7 \cdot 5 = 105$. List numbers congruent to $5 \mod 15$, and reduce them $\mod 7$ until we find one congruent to $3 \mod 7$. The numbers congruent to $5 \mod 15$ are

$$5, 20, 335, 50, 65, 80, 95, \ldots$$

Reducing mod 7, these numbers are

$$5, 6, 0, 1, 2, 3, 4$$

Since we want $3 \mod 7$, we choose 80. □

The technique used in the last example works for small numbers, but is inefficient for larger numbers. For larger numbers, we use the following technique, based on the technique in the preceding example. If $x \equiv b \mod n$, then

$$x = b + nk$$

for some integer k. So we solve

$$b + nk \equiv a \mod m$$

for k. This can be written

$$nk \equiv a - b \mod m$$

Since $(m, n) = 1$, there is a number $\overline{n}$ such that $\overline{n}n \equiv 1 \mod m$. Therefore,

$$k \equiv (a - b)\overline{n}$$

Substituting k into $b + nk$ and reducing modulo mn gives the required value of x.

Returning to the previous example, we want to find k such that $5 + 15k = 3 \mod 7$, which is the same as

$$15k = -2 \mod 7$$

Since $15 \equiv 1 \mod 7$, the inverse of 15 is 1 (or itself, since 15 and 1 are equivalent). Therefore, $k = -2 \mod 7$ so

$$x = 5 + 15(-2) \equiv -20 \mod 5 \cdot 7 \equiv 80 \mod 105$$

Example 3.13 Solve $x^2 \equiv 1 \mod 35$

Solution. Note that $35 = 5 \cdot 7$. Then, using the CRT, we have

$$x^2 \equiv 1 \mod 35 \Leftrightarrow \begin{cases} x^2 \equiv 1 \mod 7 \\ x^2 \equiv 1 \mod 5 \end{cases}$$

Now $x^2 \equiv 1 \mod 5$ has two solutions $x \equiv \pm 1 \mod 5$ and $x^2 \equiv 1 \mod 7$ also has two solutions $x \equiv \pm 1 \mod 7$

There are four different ways that these can be put together

$$\begin{aligned} x \equiv 1 \mod 5, x \equiv 1 \mod 7 &\rightarrow x \equiv 1 \mod 35 \\ x \equiv 1 \mod 5, x \equiv -1 \mod 7 &\rightarrow x \equiv 6 \mod 35 \\ x \equiv -1 \mod 5, x \equiv 1 \mod 7 &\rightarrow x \equiv 29 \mod 35 \\ x \equiv -1 \mod 5, x \equiv -1 \mod 7 &\rightarrow x \equiv 34 \mod 35 \end{aligned}$$

□

Theorem 3.34 *(Chinese Remainder Theorem, General Form) Let $m_1, \ldots, m_k$ be integers with $\gcd(m_i, m_j) = 1$ whenever $i \neq j$. Given integers $a_1, \ldots, a_k$ there exists exactly one solution $x \mod m_1 \cdots m_k$ to the simultaneous congruences*

$$x \equiv a_1 \mod m_1, x \equiv a_2 \mod m_2, \ldots, x \equiv a_1 \mod m_1$$

3.6 Fast Exponentiation

Frequently when using modular arithmetic for cryptographic applications, we need to compute numbers of the form x^a, reduced modulo n. There are some examples of this in the homework. We can use Fermat's little theorem, along with the following technique, known as fast exponentiation. Suppose we want to compute $2^{1234} \mod 789$.

1. First approach: compute 2^{1234}, then reduce modulo 789. This is impractical. 2^{1234} is too big for Matlab.

2. Second approach: compute consecutive powers and reduce mod 789. Ie.

   Compute 2^2, reduce mod 789,

   compute $2^3 = 2^2 \cdot 2 \mod 789$ using reduced form of $2^2 \mod 789$, reduce mod 789

   compute $2^4 = 2^3 \cdot 2 \mod 789$ using reduced form of $2^3 \mod 789$, reduce mod 789

   $\vdots$

   compute $2^{n+1} = 2^n \cdot 2 \mod 789$ using reduced form of $2^n \mod 789$, reduce mod 789

   - never have to work with large numbers (good)
   - requires 1233 calculations. tractable, but still too slow for practical use. (bad)

3. Third approach: We start with $2^2 \equiv 4 \mod 789$ and repeatedly square both sides to obtain the following congruences

$$\begin{aligned} 2^4 &\equiv (2^2)^2 \equiv 4^2 \equiv 16 \\ 2^8 &\equiv (2^4)^2 \equiv 16^2 \equiv 256 \\ 2^{16} &\equiv (2^8)^2 \equiv 256^2 \equiv 49 \\ 2^{32} &\equiv (2^{16})^2 \equiv 34 \\ 2^{64} &\equiv 367 \\ 2^{128} &\equiv 559 \\ 2^{256} &\equiv 37 \\ 2^{512} &\equiv 580 \\ 2^{1024} &\equiv 256 \end{aligned}$$

   Next, we write 1234 (the exponent) as a sum of powers of 2,

$$1234 = 1024 + 128 + 64 + 16 + 2$$

   Then

$$\begin{aligned} 2^{1234} &= 2^{1024+128+64+16+2} \\ &= 2^{1024}2^{128}2^{64}2^{16}2^2 \\ &\equiv 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \mod 789 \end{aligned}$$

The third approach can be generalized, providing a method for computing $a^b \mod n$ in at most $2\log_2(b)$ multiplications $\mod n$, and we never have to work with numbers larger than $(n-1)^2$. The algorithm is as follows,

1. Write b as a sum of powers of 2,

$$b = b_m 2^n + b_{m-1} 2^{n-1} + \cdots + b_1 2 + b_0$$

for some $m \in \mathbb{Z}$, $b_i \in \{0, 1\}$ (there is a unique way to do this).

2. Recursively compute a^{2^i} for $1 \leq i \leq m$, reduced modulo n at each step,

$$a^{2^{i+1}} = (a^{2^i})^2 = {a_i}^2 \mod n$$

where $a_i \equiv a^{2^i} \mod n$ and $a_i \in \{0, \ldots, n-1\}$

3. Then

$$\begin{aligned} a^b &= a^{b_m 2^m + b_{m-1} 2^{m-1} + \cdots + b_1 2 + b_0} \\ &= a^{b_m 2^m} a^{b_{m-1} 2^{m-1}} \cdot \cdots \cdot a^{b_1 2} + a^{b_0} \\ &\equiv a_m^{b_m} a_{m-1}^{b_{m-1}} \cdot \ldots \cdot a_1^{b_1} a_0^{b_0} \mod n \end{aligned}$$

The amount work needed can sometimes be further reduced using Fermat's last Theorem (or Euler's generalization).

Recall,

$$a^{p-1} \equiv 1 \mod p$$

when p is a prime and $(a, p) = 1$, and more generally,

$$a^{\phi n} \equiv 1 \mod n$$

when $(a, n) = 1$. Since $b = q(p-1) + r$ for some q, r, $0 \leq r < p-1$, we have

$$\begin{aligned} a^b = a^{q(p-1)} a^r &= (a^{p-1})^q a^r \mod p \\ &\equiv 1^q a^r \mod p \qquad \text{Since } a^{p-1} \equiv 1 \mod p \\ &\equiv a^r \mod p \end{aligned}$$

Thus, if $n = p$, then we can then apply the method above using r instead of b. When n is not prime, we can use Euler's generalization to obtain a similar result.

Chapter 4

Modern Cryptosystems

We now have the mathematics tools to describe the modern cryptographic schemes.

4.1 The RSA scheme

Historically speaking, the RSA scheme is first of the modern cryptographic systems. Unlike the classical cryptosytems, the RSA scheme is a public key cryptosytem. This means that there is a key that is distributed publicly that can be use to encrypt messages. Only the intended recipient can decrypt the message using a secret key. The method was developed by Rivest, Shamir, and Adelman in 1978. In fact it was known before then by the British Military, but it was never published (not surprisingly).

1. **key**
   (a) Alice chooses two secret prime numbers p and q.
   (b) Alice choose e such that $(e, p-1, q-1) = 1$.
   (c) Alice computes $d = \overline{e} \bmod (p-1)(q-1)$
      - Alice's public key is $n = pq$ and e
      - Alice's secret key is p, q, d and $\phi(n) = (p-1)(q-1)$
2. **Encryption** Bob encrypts a message m, where $0 \leq m < n$ as $c :\equiv m^e \bmod n$

$$m \mapsto c \equiv m^e \bmod n$$

3. **Decryption** Alice decrypts via $m \equiv c^d \bmod n$

$$c \mapsto m \equiv c^d \bmod n$$

Why this works

$$c^d \equiv (m^e)^d \equiv m^{ed} \bmod n$$

Now, since $d \equiv \overline{e} \bmod (p-1)(q-1)$, $ed \equiv 1 \bmod (p-1)(q-1)$. Therefore, by the definition of congruence, $ed = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{Z}$, so

$$\begin{aligned} c^d &\equiv m^{ed} \bmod n \\ &\equiv m[m^{(p-1)(q-1)}]^k \bmod n \quad \text{Since } ed = 1 + k(p-1)(q-1) \\ &\equiv m[m^{\phi(n)}]^k \bmod n \\ &\equiv m \cdot 1^k \bmod n \\ &\equiv m \end{aligned}$$

Example 4.1 Suppose that $p = 17$ and $q = 43$, and let $e = 29$. Then $n = pq = 731$. Also, $\gcd(17-1, 43-1, 29) = 1$. The public key is then $n = 731$ and $e = 29$. To complete the private key, Alice needs to find $d \equiv \overline{e} = \overline{29} \bmod 672$. To do this, she uses the extended Euclidean algorithm.

$$\begin{aligned} 672 &= 23 \cdot 29 + 5 \\ 29 &= 5 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \end{aligned}$$

Therefore,

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1(29 - 5 \cdot 5) = 6 \cdot 5 - 1 \cdot 29 \\ &= 6(672 - 23 \cdot 29) - 1 \cdot 29 \\ &= 6(672) - 139(29) \end{aligned}$$

Therefore, $29(-139) \equiv 1 \bmod 672$, so $d = \overline{29} \equiv -139 \equiv 533 \bmod 672$

The plaintext space is $\{m | 0 \leq m \leq 730\}$. Note that $26^2 = 676 < 730$, so we can use $\{m | 0 \leq m \leq 675\}$ instead, to map pairs of letters to numbers (with a little extra room left over).

To encrypt, we map the letter pair $(\alpha, \beta) \mapsto m = 26\alpha + \beta \mapsto c :\equiv m^e \bmod 731$

For example, $hi \mapsto (7, 8) \mapsto 26 \cdot 7 + 8 = m \mapsto m^{29}$. We use the method of fast exponentiation to compute m^{29}. First, we write the exponent 29 as a sum of powers of 2,

$$29 = 16 + 8 + 4 + 1$$

Then we square repeatedly, reducing modulo 731 at each step.

$$\begin{aligned} 29^2 &\equiv 281 \bmod 731 \\ 29^4 \equiv (29^2)^2 &\equiv 13 \\ 29^8 &\equiv 169 \\ 29^{16} &\equiv 52 \end{aligned}$$

Thus,

$$\begin{aligned} c = m^{29} &\equiv 190^{29} = 190^{16+8+4+1} \\ &= (190)^{16}(190)^{8}(190)^{4}(190)^{1} \\ &\equiv (52)(169)(13)(190) \\ &\equiv (16)(13)(190) \equiv 208(190) \\ &\equiv 46 \bmod 731 \end{aligned}$$

So the encrypted message sent is 46.

To decrypt, Alice computes $m = c^d = c^{533}$. Using fast exponentiation (as an exercise, fill in the details),

$$\begin{aligned} m &= c^{533} \equiv 46^{533} \\ &= (46)^{512}(46)^{16}(46)^{4}(46) \\ &= (154)(324)(81)(46) \\ &= 190 \bmod 731 \end{aligned}$$

Then $190 = 26\alpha + \beta$ for some numbers α and β. In fact, α is the quotient and β remainder on division of 190 by 26. Thus $\alpha = 7$ and $\beta = 8$, giving the plaintext hi.

4.2 Miller-Rabin Primality Test

Recall the following lemma,

Lemma 4.1 *If p is prime, then*

$$x^2 \equiv 1 \bmod p \Leftrightarrow x \equiv x \equiv \pm 1 \bmod p$$

Note: This can fail for composite numbers. For example, $9^2 = 81 \equiv 1 \bmod 20$ but $9 \not\equiv \pm 1 \bmod 20$.

We use this property to distinguish primes. Take a number n and write $n - 1 = 2^k m$ where m is odd. Let $1 < a < n - 1$. If n is prime, then $a^{n-1} = a^{2^k m} \equiv 1 \bmod n$. Therefore, $b_{k-1} = a^{2^{k-1}m}$ satisfies $b_{k-1}^2 \equiv 1 \bmod n$ (if n is prime).

If $b_{k-1} \equiv 1 \bmod n$, we consider $b_{k-2} = a^{2^{k-2}m} \bmod n$, etc.

Thus, we have

$$b_0 \equiv a^m, b_1 = (b_0)^2 \equiv a^{2m}, b_2 = (b_1)^2 \equiv a^{4m}, \ldots, b_k = (b_{k-1})2 \equiv a^{2^k m} = a^{n-1}$$

If n is prime, the sequence $b_0, b_1, \ldots, b_k \bmod n$ ends with a sequence of 1's, $b_t = b_{t+1} = \cdots b_k = 1$. Either $t = 0$ or $b_{t-1} = -1$.

The M-R test checks wether this happens. The algorithm is as follows,

- Choose $1 < a < n-1$ (at random, or $a = 2$, or...)
- Form the sequence

$$b_0 \equiv a^m, b \equiv (b_0)^2, b_2 \equiv (b_1)^2, \ldots, b_k \equiv (b_{k-1})^2$$

- Find the smallest t such that $b_{t+1} \equiv 1 \bmod n$
  - If there is no such t, then n is composite ($b_k \equiv 1$ if n is prime).
  - If $b_0 \equiv 1 \bmod n$, then n passes the M-R test and is "probably" prime.
  - If $t + 1 \geq 1$ and $b_t \equiv -1 \bmod n$, then n passes the M-R test and n "probably" prime.
  - If $b_{t+1} \equiv 1$ and $b_t \not\equiv \pm 1$ then n is composite.

Fact: If n passes the test for 1 choice of a, then the probability that this was wrong and n is really composite is $< 1/4$. Therefore, if we apply the test r times and n passes all r tests, the probability that the test is wrong and n is composite is $< (1/4)^r$.

Note: The smallest composite number n which passes the test for $a = 2, 3, 5, 7, 11, 13, 17, 19$ satisfies $n > 10^{14}$ (n is known)

Example 4.2 $n = 561$, $a = 2$. Then $561 - 1 = 16(35) = 2^4 \cdot 35$. Using fast exponentiation,

$$\begin{aligned} 2^{35} &\equiv 263 \bmod 561 \\ 2^{70} &\equiv 166 \\ 2^{140} &\equiv 67 \\ 2^{280} &\equiv 1 \end{aligned}$$

Because $2^{280} \equiv 1$, but $2^{140} \not\equiv \pm 1$, n fails the M-R test and 561 is composite.

4.3 Analysis of Attacks

In practice, the primes p and q in the RSA scheme are chosen to be very large, about 100 digits (in base 10 notation). Then $\phi(n) = (p-1)(q-1)$ is about 200 digits long, which makes $\phi(n)$ hard to factor. Thus, we assume that it is "hard" to factor n and ask what Eve can do given this assumption.

Eve knows n, e, and c. She does not know p, q, and d.

Claim 1 If Eve knows n and $\phi(n)$

1. She can factor n

2. She can find d.

Proof.

1. $n - \phi(n) + 1 = pq - (p-1)(q-1) + 1 = p + q$. Therefore, Eve knows pq and $p + q$. The polynomial

$$x^2 - (n - \phi(n) + 1)x + n = x^2 - (p+q)x + pq$$

has roots p and q. But these can easily be determined from the quadratic formula

2. Use the method Alice used to find d.

□

Summary: Assuming Eve cannot factor n implies Eve cannot find $\phi(n)$.

Example 4.3 If Eve knows $n = 221$ and $\phi(n) = 192$, she considers $x^2 - (221 - 192 + 1)x + 221 = x^2 - 30 + 221$. Then, by the quadratic polynomial,

$$p, q = \frac{30 \pm \sqrt{900 - 4(221)}}{2} = 13, 17$$

Claim 2 If Eve knows d and e, then she can probably factor n.

Proof. Recall that $ed \equiv 1 \bmod \phi(n)$, so $de = k\phi(n) + 1$ for some k. Thus,

$$a^{de-1} = (a^{\phi(n)})^k \equiv 1 \bmod n$$

for all a with $(a, n) = 1$. This means Eve can use the Method for Universal Exponents to factor n. □

4.3.1 Universal Exponent Factorization Method

This method is based on the same principles as the Miller-Rabin algorithm, but rather than testing to see if a number is prime, the method is used to find factors.

Suppose $r > 0$ is such that $a^r \equiv 1 \bmod n$ for all a with $(a, n) = 1$. (Such an r always exists. For example, $r = \phi(n)$)

- Write $r = 2^k m$ with m odd.

- Choose a random value a with $1 < a < n - 1$.
- If $(a, n) \neq 1$, we have a factor of n and so we may assume that $(a, n) = 1$.
- Set $b_0 := a^m \bmod n$ and $b_{j+1} := b_j^2 \bmod n$ for $1 \leq j \leq k - 1$
- If $b_0 \equiv 1 \bmod n$ then stop and choose a new a
- If $b_j \equiv -1 \bmod n$ for some j then stop and choose a new a
- Otherwise, there is a number j such that

$$b_j \not\equiv \pm 1 \bmod n, \quad \text{but} \quad b_{j+1} \equiv 1 \bmod n$$

Then $n|(b_j^2 - 1) = (b_j - 1)(b_j + 1)$, so $\gcd(b_j - 1, n)$ gives a non-trivial factor of n. Using a few values of a, we have a high probability of factoring n.

Example 4.4 $13^2 \equiv 3^2 \bmod 40$, but $13 \not\equiv \pm 3 \bmod 40$, so 40 is composite.

4.3.2 Trial Division

Suppose n has 100 decimal digits. Then $\sqrt{n} \approx \sqrt{10^{100}} = 10^{50}$. By the Prime Number Theorem, there are approximately

$$\frac{10^{50}}{\ln(10^5 0)} = \frac{10^{50}}{50 \ln 10} = \frac{10^{50}}{115.1} \approx 8.18 \times 10^{47} = 10^{48}$$

prime numbers less than 10^{50}.

It takes 160 bits or 20 bytes to store a 48 digit number. THus, to store the list of primes less than 10^{50} would take

$$20 \times 10^{48} = 2 \times 10^{49}$$

bytes. This would take 2×10^{37} 1 terabyte hard drives.

4.3.3 Common Modulus Protocol Failure

Suppose that Frank and Bob use the same modulus, $n = pq$ but different public exponents e_F and e_B. Alice encrypts the same message m to both Bob and Frank. Assuming $(m, n) = 1$, Eve may easily decode: she finds a and b such that $ae_F + be_B = 1$. Then

$$(c_F)^a (c_B)^b = (m^{e_F})^a (m^{e_B})^b = m^{ae_F + be_B} \equiv m^1 \bmod n$$

4.3.4 Small Decryption Exponent Attack

Theorem 4.2 *Let p, q be prime with $q < p < 2p$ and let $n = pq$. Suppose $d < \frac{1}{3}n^{1/4}$. Given n and e such that $de \equiv 1 \bmod \phi(n)$ there is an efficient procedure for computing d.*

- This produced uses continued fractions for e/n.
- Conclusion
  1. p and q should be slightly different sizes.
  2. d should be large.

4.3.5 Partial Disclosure Attack

Theorem 4.3 *Let $n = pq$ have r digits. If we know the first $r/4$ or the last $r/4$ digits of p, we can efficiently factor n.*

Theorem 4.4 *Suppose n and e form an RSA public key and n has r digits. Let d be the decryption exponent. If we know the last $r/4$ digits of d we can efficiently find d in time that is linear in $e \log_2 e$*

- This is useful if e is small. If $e \approx n$, this is not useful.

4.4 Factorization Methods

We now consider various factorization methods and their relevance to the RSA scheme.

4.4.1 Fermat Factorization

Here, we try to express n as a difference of squares, $n = x^2 - y^2$. Then $n = (x - y)(x + y)$.

Example 4.5 To factor $n = 295927$, we compute

$$n + 1^2, n + 2^2, n + 3^3, \ldots$$

until we find a square. Here, $295927 + 3^2 = 295936 = (544)^2$. Therefore,

$$\begin{aligned} n = 295927 &= (544)^2 - (3)^3 \\ &= (544 - 3)(544 + 3) = (541)(547) \end{aligned}$$

This method works well if $n = pq$. where $|p - q|$ is small. It takes $\frac{1}{2}|p - q|$ steps to find a factorization of n.

For this reason, p and q are chosen in RSA with $|p - q|$ not too small.

If p and q are both random 100 digits primes, then $|p - q|$ will also be 100 digits.

4.4.2 Pollard's $p - 1$ Factoring Algorithm (to factor $n - 1$)

1. Choose an integer $a > 1$ (Often $a = 2$).
2. Choose a bound B.
3. Compute $b \equiv a^{B!}$ $(b_1 \equiv a, b_{i+1} = b_i^{i+1}, b_B = b)$
4. Let $g = (b - 1, n)$.
5. If $g > 1$, we have a non-trivial factor of n.

Why this works

Suppose p is a prime factor of n such that $p - 1$ has only small ($\leq B$) prime factor. Then, probably, $p-1|B!$, so $B! = (p-1)k$ for some k. Then $b \equiv a^{B!} \equiv (a^{p-1})^k \equiv 1 \bmod p$ Therefore, $p|((b - a), n) = g$

What if $(b - 1, n) = n$. If q is another prime factor of n it is unlikely $b \equiv 1 \bmod q$ (unless $q - 1$ has only small prime factors), thus $(b - 1, n)$ is probably not n.

Even if $g = n$, we ma still proceed, for in this case, we know a and $r = B!$ such that $a^r \equiv 1 \bmod n$. Therefore, we may apply the exponent factorization method

Or, we may repeat the above method with a smaller value of B.

Conclusion For RSA with $n = pq$, we want both $p-1$ and $q-1$ to have large prime factors.

We may do this as follows. Suppose we want p to have 100 digits. Choose a large prime p_0, say with 40 digits. Consider integers of the form $kp_0 + 1$ with $k \approx 10^{60}$. Use Miller-Rabin to find a prime number of the form $kp_0 + 1$. On average, this should take less than 100 steps to find $kp_0 + 1$ primes.

4.5 Quadratic Sieve

Proposition 4.5 *Suppose* $x^2 \equiv y^2 \bmod n$ *but* $x \not\equiv \pm y \bmod n$ *then* n *is composite. Moreover,* $(x - y, n)$ *is a nontrivial factor of* n

Proof. Set $d := (x - y, n)$. Then $d \neq n$ since $x \neq y \bmod n$. Suppose that $d = 1$. Since $n|(x-y)(x+y)$, $(x-y, n) = 1$ means that $n|x+y$, and so $x =\equiv -y$, which is a contradiction. □

Suppose we want to factor $n = 3837523$. Observe,

$$\begin{aligned} 9398^2 &\equiv 5^5 \cdot 19 \bmod n \\ 190095^2 &\equiv 2^2 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \bmod n \\ 1954^2 &\equiv 3^2 \cdot 3^2 \cdot 13^3 \bmod n \\ 17078^2 &\equiv 2^6 \cdot 3^2 \cdot 11 \end{aligned}$$

Multiply these together,

$$\begin{aligned} (9398 \cdot 19095 \cdot 1964 \cdot 17078)^2 &\equiv (2^4 \cdot 3^2 \cdot 5^3 \cdot 11 \cdot 13 \cdot 19)^2 \bmod n \\ \text{i.e.} \quad (2230382)^2 &\equiv (2586705)^2 \bmod n \\ \text{But} \quad 2230387 &\not\equiv \pm(2586705) \bmod n \end{aligned}$$

$(2230387 - 2586705, n) = 1093$ $n = (1093)(3511)$

How did we do this?

1. Find numbers m such that $m^2 \bmod n$ has only small prime factors ("small" : $< B$ in factor base). For example, in the previous example, the factor base is $\{2, 3, 5, 7, 11, 13, 17, 19\}$ and $B = 20$.
2. List the resulting relations as rows in a matrix

	2	3	5	7	11	13	17	19
9398	0	0	5	0	0	0	0	1
19095	2	0	1	0	1	1	0	1
1964	0	2	0	0	0	3	0	0
17078	6	2	0	0	1	0	0	0
8077	1	0	0	0	0	0	0	1
3397	5	0	1	0	0	2	0	0
14262	0	0	2	2	0	1	0	0

Now, look for mod2 relations among the rows. Here are 3 such relations,

1. $R_1 + R_5 + R_6 \equiv \mathbf{0} \bmod 2$
2. $R_1 + R_2 + R_3 + R_4 \equiv \mathbf{0} \bmod 2$
3. $R_3 + R_7 \equiv \mathbf{0} \bmod 2$

Each such relation among the rows expresses a congruence of squares mod$n$.

1. $(9398 \cdot 8077 \cdot 3397)^2 \equiv 2^6 \cdot 2^6 \cdot 13^2 \cdot 19^2$
2. $(9398 \cdot 19095 \cdot 1964 \cdot 17078)^2 \equiv (2^3 \cdot 3^2 \cdot 5^3 \cdot 11 \cdot 13^2 \cdot 19)^2$
3. $(1964 \cdot 14262)^2 \equiv (3 \cdot 5 \cdot 7 \cdot 13^2)^2$

Thus we have 3 expressions $x^2 \equiv y^2 \bmod n$. If $x \not\equiv \pm y \bmod n$, then $\gcd(x-y, n)$ yields a nontrivial factor of n. If $x \equiv \pm y$ then $\gcd(x-y, n) = 1$ and we get nothing. Of the three give relations,

1. $(35905233)^2 \equiv (247000)^2$, but $3590523 \equiv -247000$, so we get nothing.
2. $(2230387)^2 \equiv (2586705)^2$ and $\gcd(2230387 - 2586705, n) = 1093$
3. $(1147907)^2 \equiv (17745)^2$, and $\gcd(1147907 - 17745, n) = 1093$

Now we consider how we find squares whose residues have only small factors.

The idea is to find numbers m such that m^2 is slightly larger than some multiple of n. To do this, we take $m = [\sqrt{in} + j]$ for j small. Then $m^2 \approx in + 2j\sqrt{in} + j^2 \approx 2j\sqrt{in} + j^2 \bmod n$. If i is not too large, this number is fairly small and so there is a good chance it will have only small prime factors. For example $8077 = [\sqrt{17n} + 1]$ and $9398 = [\sqrt{23n} + 4]$. This method is the basis of the best known public factoring method (NFS). The main problem is to find relations of the form $x^2 \equiv$ Product of Small Primes mod n

- An improved version of this method is called the *quadratic sieve*
- A further improvement is a new method called the number field sieve
- Every non-trivial relation $x^2 \equiv y^2$ yields $x \equiv \pm y$ at most half the time. Thus, if we have many relations, (say the matrix has several more rows than columns), we have a good chance of factoring n.

In 1978, when RSA was made public, the authors publicized an n with 129 digits and $e = 9007$ and a ciphertext and challenged people to break it.

At that time, they estimated it would take 4×10^{16} years using 1978 methods to factor n. They risked offering a \$100 prize for the first decryption done before April 1, 1982.

In 1994, Atkins, Graff, Lenstra, and Leyland factored n.

They used a factor base of 524339 "small" primes. i.e. all primes less than $B = 16333610$, (plus two "large" primes between 16333610 and 2^{30}). The Birthday Paradox (see below) implies that there should be several cases where the same large prime occurs in more than 1 relation.

Six hundred people using 1600 computers found congruences of the desired type. These were emailed to a central machine which verified them and removed duplicates.

Over 7 months they obtained a matrix with 524339 column and 569466 rows. The matrix was sparse. Using Gaussian Elimination, this was reduced to a non-sparse 188614×188160 matrix in 12 hours. 45 more ours produced 205 dependencies. The first 3 yielded trivial factorizations. the 4th factor n and gave them the plaintext "the magic words are the squeamish ossifrage"

4.6 Pollard Rho

4.6.1 Random Sequences

Suppose you have a 20-sided (fair) die, with faces numbered from 1 to 20. Throw the die repeatedly to get a sequence

$$x_0, x_1, x_2 \ldots, ...$$

of integers in the range $1 \leq x_i \leq 20$. Eventually, the number that appears after a roll of the dice will be the same as an earlier roll. That is, There is an integer k such that

- $x_0, x_1, \ldots, x_{x-1}$ are all distinct, but
- $x_k = x_j$ for some $0 \leq j < k$

Question 4.1 How large is k on average? That is, how many rolls should you expect to make before the first duplicate shows up?

The average (mean) value of k is 5.29 (rounded to 2 decimal places). That is, *on average* we expect the first repeat to appear somewhere near x_5.

If we replace the 20-sided die by an n-sided die, we can ask the same question: How many throws do you expect to make before the first repeat shows up? A general formula is

$$\text{Average value of } k = \sum_{j=1}^{n} \frac{n!}{n^j (n-j)!}$$

(As an exercise, show that $n!/(n^j(n-j)!)$ is the probability that the first j throws are all distinct. The formula follows.)

A very good approximation to this formula is

$$\text{Average value of } k \approx \sqrt{\frac{n\pi}{2}} - \frac{1}{3}$$

Example 4.6 (The Birthday Paradox) Let $n = 366$, the possible number of birthdays. Using the previous formula, the average value of k is around

$$\text{Average value of } k \approx \sqrt{366\pi/2} - 1/3 \approx 23.6$$

Thus, if there are 24 or more people in a room, it is likely that at least two people in the room have the same birthday.

More precisely, if there are exactly 23 people in the room, the probability of a shared birthday is

$$1 - \frac{366!}{343!36623} = 0.506$$

So the probability of a shared birthday is greater than 50%. For a room of 41 people, the probability is 90%, for 58 it's 99%.

(These results assume that each birthday is equally likely, which isn't true. Feb 29 is obviously less common than the rest, but even among the rest, certain birthdates are more common than others. Thus, the probabilities are actually underestimates.)

Example 4.7 (The Powerball) Each draw of the multi-state 'Powerball' produces 5 distinct integers in the range 1 to 55, along with a powerball number between 1 and 42. The total number of possible combinations is

$$\frac{55!}{50!5!} \cdot 42 = 146107962$$

Since there are two drawings every week, how many years would you expect the Powerball to run before a duplicate draw is made?

With $n = 146107962$, $\sqrt{n\pi/2} \approx 15419$, so a repeated drawing is expected after 15149 draws. There are 104 drawings per year, so a repeat is expected at

$$\frac{14607962}{104} \approx 148$$

years. It could happen much soon. For example, the chance that a repeat drawing occurs within 55 years is 10%.

The Pollard Rho factorization method is based on these ideas.

4.6.2 The Pollard Rho Factorization Method

Suppose that n is a composite integer. Define a sequence $x_0, x_1, x_2, \ldots$ of integers x_i in the range $0 \leq x_i < n$ recursively as follows,

$$x_0 = 0, \qquad x_{k+1} = (x_k^2 + 1) \bmod n, k \geq 1$$

(That is x_{k+1} is $x_k^2 + 1$ reduced modulo n, so that x_{k+1} is at least 0 and less than n)

Example 4.8 Suppose that $n = 527$. Then the sequence starts

$$0, 1, 2, 5, 226, 150, 367, 350, 274, \textit{etc.}$$

There are only finitely many possible values for n, so the sequence repeats eventually. Now we make the following leap of faith: The initial part of the sequence (before first repeat) behaves like a random sequence. Then we expect the first repeat somewhere around $\sqrt{n\pi/2}$.

Now let p be the smallest prime divisor of n (so $p \leq \sqrt{n}$), and define a sequence $y_0, y_1, \ldots,$ of integers by $y_i = x_i \bmod p$. Then

$$\begin{aligned} y_{k+1} &\equiv x_{k+1} \bmod p \\ &\equiv x_x^2 + 1 \bmod p \\ &\equiv y_k^2 + 1 \bmod p \end{aligned}$$

And hence $y_{k+1} = (y_k^2 + 1) \bmod p$, so the $4y_i$ obey a similar recurrence to the x_i and by the same leap of faith, we expect the sequence of y values to repeat after around $\sqrt{p\pi/2}$ steps. Note that since $p \leq \sqrt{n}$, we have $\sqrt{p\pi/2} \leq 1.26n^{1/4}$

In the example above, the smallest prime factor of n is 17, and the sequence y_i starts

$$0, 1, 2, 5, 9, 14, 10, 16, 2, 5, 9, \ldots$$

Here is the key observation: even though we don't know what p is, we can detect when the sequence y_i starts to repeat. For any indices j and k,

$$\begin{aligned} y_j = y_k &\Rightarrow x_j \equiv x_k \bmod p \\ &\Rightarrow p|(x_k - x_j) \end{aligned}$$

Since $p|n$, we have

$$p|\gcd(x_k - x_j, n)$$

In particular, it follows that

$$y_j = y_k \Rightarrow \gcd(x_k - x_j, n) \neq 1$$

As long as $x_k \neq x_j$, $\gcd(x_k - x_j, n)$ must be a *proper* (not equal to n) *nontrivial* (not equal to 1) factor of n.

This suggests the following algorithm,

- Compute the sequence $x_0, x_1, \ldots$ as above
- For each x_k, calculate
$$g = \gcd(x_k - x_j, n),\ 0 \leq j < k$$
until values of j and k are found for which $g \neq 1$. Then $\gcd(x_k - x_j, n)$ is (hopefully) a proper factor of n

We expect the first successful value of k to be of the same order of magnitude as $\sqrt{p\pi/2}$.

In the example above, with $n = 527$, we find that $\gcd(x_5 - x_4) = 31$, from which the factorization $527 = 31 \cdot 17$

This not practical because,

- Large amount of storage for x_k values.
- Requires cp steps (c a constant), making the algorithm no better than trial division.

We can make the Pollard-Rho method practical with the help of the following Lemma

Lemma 4.6 *Suppose that $y_j = y_k$ for some $0 \leq j < k$. Let m be the smallest positive multiple of $k - j$ for which $m \geq j$. Then $m \leq k$ and $y_m = y_2 m$. Hence $\gcd(x_{2m} - x_m, n) \neq 1$ is a nontrivial factor of n.*

We then have the **Pollard Rho algorithm**

Suppose n is a composite integer. To factorize n.

1. Set $x_0 = 0$. For each k
2. Compute $x_k = (x_{k-1}^2 + 1) \bmod n$
3. Compute $x_{2k} = (((x_{2k-2}^2 + 1) \bmod n) + 1) \bmod n$
4. Compute $g = \gcd(x_{2k} - x_k, n)$. If $g \neq 1$, stop: g is a nontrivial factor of n. Otherwise, try the next k.

When the algorithm terminates, g will be a nontrivial factor of n.

Using $n = 527$ again (as in the previous examples)

Example 4.9

k	x_k	x_{2k}	$\gcd(x_{2k} - x_k, 527)$
0	0	0	527
1	1	2	1
2	2	26	1
3	5	367	1
4	26	274	31

Thus, the Pollard-Rho shows that 31 is a factor of n.

4.7 Discrete Logarithms and ElGamel Encryption

Let p be a fixed prime and let α and β be integers modulo p. The problem of finding an integer x such that

$$\beta \equiv \alpha^x \bmod p$$

(if one exists) is called the *discrete logarithm problem*. In general, if there is a solution x, then will be more than one solution. However, if n is the smallest possible integer such that $\alpha^n \equiv 1 \bmod p$, then we may assume that $0 \leq x < n$. In that case, we denote

$$x = L_\alpha(\beta)$$

and call x the *discrete logarithm* of β with respect to α. The prime p is omitted from the notation (and is usually clear from context).

Example 4.10 Let $p = 11$ and let $\alpha = 2$. Since $2^6 = 9 \bmod 11$, $x = 6$ is a solution to

$$2^x \equiv 9 \bmod p$$

Therefore, $L_2(9) \leq 6$. But the smallest positive integer n such that $2^n = 1$ is $n = 10$ (by inspection), and $0 \leq 6 < 10$, so $L_2(9) = 6$.

Note that $x = 16$ and $x = 26$ are also solutions, but $x > 10$ in both cases so neither 16 nor 26 are the discrete logarithm.

Let α be an integer modulo p. If

$$\beta \equiv \alpha^x \bmod p$$

has a solution for every integer β modulo p, then α is called a *primitive root* modulo p.

Example 4.11

1. The nonzero powers of 2 modulo 7 are

   $$2^1 = 2, 2^2 = 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1$$

   $2^x \not\equiv 3, 5$ for any number x, so 2 is not a primitive root mod 7.

2. The nonzero powers of 3 modulo 7 are

   $$3^1 = 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 = 5, 3^6 = 1$$

   Each nonzero integer β mod 7 can be written as 2^x for some x, so 3 is a primitive root mod 7.

Often α is taken to be a primitive root modulo p. The discrete log behaves in many ways like the usual logarithm. For example, if α is a primitive root modulo p, then

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2)$$

When p is small, discrete logs can be found by an exhaustive search. When p is large, this is not feasible. It is believed that computing discrete logs is hard in general, which is the basis of several cryptosystems.

4.8 The ElGamel Public Key Cryptosystem

Plaintexts: Integers modulo p

Ciphertexts: pairs of integers (r, t) mod p.

Suppose Alice wants to send a message m to Bob.

Bob constructs a public key as follows. Bob

1. Chooses
   (a) A large prime p
   (b) A primitive root α
   (c) A secret integer a
2. Computes $\beta \equiv \alpha^a \bmod p$
3. Publishes (p, α, β)

To encrypt, Alice

1. Downloads (p, α, β)
2. Chooses a secret random intger k and computes $r = \alpha^k \bmod p$
3. Computes $t = \beta^k m \bmod p$
4. Sends the pair (r, t) to Bob

To Decrypt, Bob computes

$$tr^{-a} \equiv m \bmod p$$

Why this works

$$tr^{-a} \equiv \beta^k m(a^x)^{-a} \equiv (\alpha^a)^k m\alpha^{-ak} \equiv m \bmod p$$

Security

If Eve determines a, then she can decrypt by the same procedure as Bob. The number $x = a$ is a solution to the congruence

$$\beta \equiv \alpha^x \bmod p$$

That is, $a = L_\alpha(\beta)$. Since it is difficult to compute discrete logs, a is kept secure.

If Eve finds k, she can decrypt by computing $t\beta^{-k} \equiv m$. But the number k is also a discrete logarithm $L_\alpha(r)$, so it is secure.

Suppose that Alice sends messages m_1 and m_2 to Bob using the same value of k for both messages. Then $r = \alpha^k$ for both messages and

$$t_1 = \beta^k m_1 \qquad \text{and} \qquad t_2 = \beta^k m_2$$

so the ciphertexts are (r, t_1) and (r, t_2). Note that

$$\frac{t_1}{m_1} \equiv \beta^k \equiv \frac{t_2}{m_2}$$

so

$$m_2 \equiv t_2 \frac{m_1}{t_1} \bmod p$$

Thus, if Eve determines m_1, she can determine m_2. Therefore, it is essential that different values of k are used for different messages.

4.8.1 Computing Discrete Logarithms

For simplicity, we assume that α is a primitive root mod$p$, so $p-1$ is the smallest positive exponent n such that $\alpha^n = 1 \bmod p$. This means that

$$\alpha^{m_1} \equiv \alpha^{m_2} \Leftrightarrow m_1 \equiv m_2 \bmod p-1$$

Suppose that

$$\beta \equiv \alpha^x, \quad 0 \leq x < p-1$$

The Pohlig-Helman Algorithm

We can use the following method when the prime factors of $p-1$ are small.

To find the discrete logarithm $L_\alpha(\beta)$ modulo p,

1. Factor $p-1$ into prime powers
$$p-1 = \prod_i q_i^{r_i}$$
where the q_i are distinct.

2. For each factor $q_i^{r_i}$ compute the discrete logarithm modulo $q_i^{r_i}$ (if possible). That is, we find a_i such that
$$a_i \equiv L_\alpha(\beta) \bmod q_i^{r_i}$$

3. Recombine using the Chinese Remainder Theorem to find $x = L_\alpha(\beta)$.

$$\begin{aligned} x &\equiv a_1 \bmod q_1^{r_1} \\ x &\equiv a_2 \bmod q_2^{r_2} \\ x &\equiv a_3 \bmod q_3^{r_3} \\ &\vdots \end{aligned}$$

(The Chinese Remainder Theorem guarantees that there is a unique number x satisfying all of these equations, up to congruence modulo $p-1$.)

Steps 1 and 3 have already been covered in earlier sections. We now see how to do step 2. Suppose that $q^r = q_i^{r_i}$. We write

$$x = x_0 + x_1 q + x_2 q^2 + \ldots + x_{r-1} q^{r-1}, \qquad 0 \le x_i \le q-1$$

and successively determine the coefficients $x_0, x_1, \ldots, x_{r-1}$

Note that

$$\begin{aligned} x\left(\frac{p-1}{q}\right) &= x_0\left(\frac{p-1}{q}\right) + (p-1)(x_1 + x_2 q + x_3 q^2 + \ldots) \\ &= x_0\left(\frac{p-1}{q}\right) + (p-1)n \end{aligned}$$

For some integer n. Now raise both sides of the congruence $\beta \equiv \alpha^x$ to the $(p-1)/q$ to obtain

$$\beta^{(p-1)/q} \equiv \alpha^{x(p-1)/q} \equiv \alpha^{x_0(p-1)/q}(\alpha^{p-1})^n \equiv (\alpha^{(p-1)q})^{x_0} \bmod p$$

The last congruence follows from Fermat's Little Theorem. To find x_0, we use an exhaustive search, looking at powers

$$(\alpha^{(p-1)/q})^k \bmod p, \quad k = 0, 1, 2, \ldots, q-1$$

until some k yields $\beta^{(p-1)/q}$. Then $x_0 = k$. Suppose, now, that $q^2 | p-1$. Let

$$\beta_1 \equiv \beta\alpha^{-x_0} \equiv \alpha^{q(x_1 + x_2 q + \cdots)} \bmod p$$

Raise both sides to the $(p-1)/q^2$,

$$\begin{aligned} \beta_1^{(p-1)/q^2} &\equiv \alpha^{(p-1)(x_1 + x_2 q + \cdots)/q} \\ &\equiv \alpha^{(p-1)/q}(\alpha^{p-1})^{x_2 + x_3 q + \cdots} \\ &\equiv (\alpha^{(p-1)/q})^{x_1} \bmod p \end{aligned}$$

where, again, the last congruence follows from Fermat's Little Theorem and we can use an exhaustive search to find x_1.

In general, to find $x_0, x_1, x_2 \ldots$, we do the following.

Let $\beta_0 = \beta$. For each $i \ge 1$ such that $q^{i+1} | p-1$.

1. Let
$$\beta_i = \beta_{i-1}\alpha^{-x_{i-1}}/q^{i-1}$$
2. Find k such that
$$(\alpha^{(p-1)/q})^k = \beta_i^{(p-1)/q^{i+1}}, \quad k = 1, \ldots, q-1$$
using an exhaustive search.
3. Then $x_i = k$

We repeat this for all (distinct) prime factors of $p-1$.

Example 4.12 Let $p = 41, \alpha = 7$, and $\beta = 12$. We want to solve

$$7^x \equiv 12 \bmod 41$$

Solution. First, we factor $p - 1 = 41 - 1$ into powers of distinct primes

$$40 = 2^3 \cdot 5$$

Thus, we need to find

$$x \bmod 2^3$$

and

$$x \bmod 5$$

We find x mod 8 first. Write $x = x_0 + 2x_1 + 2^2x_2$ mod 8 (Note: for each of x_0, x_1, and x_2, there are only 2 possible values, 0 or 1). First, find x_0,

$$\beta^{(p-1)/2} \equiv 12^{20} \equiv 40 \equiv -1 \bmod 41$$

and

$$\alpha^{(p-1)/2} \equiv 7^{20} \equiv -1 \bmod 41$$

Since

$$\beta^{(p-1)/2} \equiv (\alpha^{(p-1)/2})^{x_0}$$

we have $x_0 = 1$. Next,

$$\beta_1 \equiv \beta\alpha^{-x_0} \equiv 12 \cdot 7^{-1} \equiv 31 \bmod 41$$

Also,

$$\beta_1^{(p-1)/(2^2)} \equiv 31^{10} \equiv 1 \bmod 41$$

Since

$$\beta_1^{(p-1)/(2^2)} \equiv (\alpha^{(p-1)/2})^{x_1} \bmod 41$$

we have $x_1 = 0$. Continuing, we have

$$\beta_2 \equiv \beta_1\alpha^{-2x_1} \equiv 31 \cdot 7^0 \equiv 31 \bmod 41$$

and

$$\beta_2^{(p-1)/q^3} \equiv 31^5 \equiv -1 \equiv (\alpha^{(p-1)/2})^{x_2} \bmod 41$$

Therefore, $x_2 = 1$. We have obtained

$$x \equiv x_0 + 2x_1 + 4x_2 \equiv 1 + 4 \equiv 5 \bmod 8$$

Now, we let $q = 5$ and find x mod 5. We have

$$\beta^{(p-1)/5} \equiv 12^8 \equiv 18 \bmod 41$$

and

$$\alpha^{(p-1)/q} \equiv 7^8 \equiv 37 \bmod 41$$

Trying the possible values of k yields

$$37^0 \equiv 1,\ 37^1 \equiv 37,\ 37^2 \equiv 16,\ 37^3 \equiv 18,\ 37^4 \equiv 10,\ \bmod 41$$

Therefore, 37^3 gives the desired answer, so $x \equiv 3 \bmod 5$.

By the Chinese Remainder Theorem, there is a unique x such that

$$x \equiv 5 \bmod 8 \qquad \text{and} \qquad x \equiv 3 \bmod 5$$

Using the technique from Chapter 3, we find that $x \equiv 13 \bmod 41$. A quick calculation shows that

$$7^{13} \equiv 12\ .$$

□

4.9 Data Encryption Standard

4.9.1 Introduction

In 1973, the US government issued a request for a cryptosystem to become the national standard. IBM submitted an algorithm called LUCIFER in 1974. The NSA reviewed it and modified it producing an algorithm that is now called the Data Encryption Standard (DES). In 1975, the National Bureau of Standards released a free licence for its use and in 1977, the NBS made it the official data encryption standard.

It is not as secure as a public key system, but it is much faster. It remained the standard until 2000.

4.9.2 A Feistel Cipher

A Feistel cipher is a simplified DES-like algorithm. We will encrypt a block of plaintext M consisting of 12 bits. We split M into two halves, $M = L_0R_0$ each with 6 bits. The secret key K has 9 bits. K is used to generate a key sequence $K = K_0, K_1, \ldots, K_n$. We repeatedly perform the same steps, each "round" transforming the 12-bit string $L_{i-1}R_{i-1}$ into the 12 bit string L_iR_i.,

$$\begin{array}{ccccccccc} (L_0, R_0) & \to & (L_1, R_1) & \to & (L_2, R_2) & \to & \cdots & \to & (L_n, R_n) \\ K = K_0 & \to & K_1 & \to & K_2 & \to & \cdots & \to & K_n \end{array}$$

In general, $(L_i, R_i) = F(L_{i-1}, R_{i-1}, K_i)$. We choose F so that

- $L_i := R_{i-1}$
- $R_i := L_{i-1} \oplus f(R_{i-1}, K_i)$. (the symbol $\oplus$ stands for XOR, equivalent to addition mod2).

where f is any function

$$f : \{0,1\}^6 \times \{0,1\}^9 \to \{0,1\}^6$$

Question: How do we decrypt (L_n, R_n) to get back to (L_0, R_0)?

Answer. Use the same algorithm with input (R_n, L_n) and the keys in the order $K_n, K_{n-1}, \ldots, K_0$.

That is,

$$\begin{aligned} (R_n, L_n) &\mapsto (L_n, R_n \oplus f(L_n, K_n)) \\ &= (R_{n-1}, L_{n-1} \oplus f(R_{n-1}, K_n) \oplus f(L_n, K_n)) \\ &= (R_{n-1}, L_{n-1} \oplus f(R_{n-1}, K_n) \oplus f(R_{n-1}, K_n)) \\ &= (R_{n-1}, L_{n-1}) \end{aligned}$$

using the substitutions $L_n = R_{n-1}$ and $R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$. Repeating another round gives

$$(R_{n-1}, L_{n-1}) \mapsto (R_{n-2}, L_{n-2})$$

and after n rounds, we are back to the original message $M = (L_0, R_0)$.

Notes:

- Decryption and Encryption are essentially the same.
- Any function f will work.
- Any sequence $K = K_0, \ldots, K_n$ of keys will work.

Some choices of f and key sequence are better than others. The K_i are usually chosen so that K_i is constructed from K_{i-1}.

Example 4.13 Suppose that $L_{i-1}R_{i-1} = 011100|100110$, $K_i = 01100101$, and

$$f(R_{i-1}, K_i) = 000100$$

as above.

$$\begin{aligned} f(R_{i-1}, K_i) \oplus L_{i-1} &= 000100 \oplus 011100 \\ &= 011000 =: R_i \end{aligned}$$

and $L_i = R_{i-1}$. Therefore $L_iR_i = 100110|011000$. This is the input for the next round.

The security of a Feistel cipher depends on f and the choice of key sequence.

4.9.3 DES

A block of plaintext is 64 bits. The key has 56 bits, but is expanded to a 64 bit string K by setting *parity bits* $b_8, b_{16}, b_{24}, \ldots, b_{64}$ so that the Hamming weights (defined below) of

$$\begin{aligned} wt(b_1, \ldots, b_8) &\equiv 1 \bmod 2 \\ wt(b_9, \ldots, b_{16}) &\equiv 1 \\ &\vdots \\ wt(b_{57}, \ldots, b_{64}) &\equiv 1 \end{aligned}$$

where $wt(v)$ is the number of 1s in v. This is done for error correcting purposes.

The ciphertext is 64 bits.

DES Algorithm

Input: m (64 bits)

Output: c (64 bits)

1. A fixed permutation $\pi \in \Sigma_{64}$ is applied to m,

$$m_0 := \pi(m)$$

2. For $1 \leq i \leq 16$

$$\begin{aligned} L_i &:= R_{i-1} \\ R_i &:= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

   where K_i is 48-bits, obtained from K.

3. Switch left and right

$$(L_{16}, R_{16}) \mapsto (R_{16}, L_{16})$$

4. Apply π^{-1}:

$$c := \pi^{-1}(R_{16}, L_{16})$$

Notes:

- Since we switch left and right in Step 3, decryption works in exactly the same way using the keys in the reverse order.
- π gives no cryptographic security and appears to have been introduced for hardware reasons. Steps 1, 3, and 4 are straightforward.

Step 2 is a Feistel Cipher of 16 rounds, which requires a key sequence K and a function f. In order to apply the algorithm then, we need to know how to compute f from R_{i-1} and K_i and we need to know how to produce K_i.

4.9.4 Finding $f(R_{i-1}, K_i)$

We use the following procedure to compute $f(R, K)$ used in the algorithm.

1. Expand R to 48 bits $R \mapsto E(R)$ (See below)
2. Compute $E(R) \oplus K = B_1|B_2|B_3|B_4|B_5|B_6|B_7|B_8$ so that each B_i is 6 bits.
3. Apply functions $S_1 \ldots, S_8$ called *S-boxes* to the B_i.
   Each S-box is a (carefully chosen) function

$$S_i : \{0,1\}^6 \to \{0,1\}^4 \qquad \text{not 1-1}$$

   (In 1974, the largest S-box that would fit on 1 chip was 6-input bits and 4-output bits)
   Let

$$C_i = S_i(B_i), \quad 1 \leq i \leq 8$$

   This gives

$$C = C_1 C_2 \ldots C_8 =: f(R, K) \qquad (32 bits)$$

4. (Different sources say different things at this point. In one source, including the textbook for this course, a permutation is applied to C, in others, this step is absent.)

S-boxes are chosen so that

1. they are highly non-linear
2. S_i is onto
3. If two inputs differ in only 1 spot, then their outputs must differ in at least 2 bits
4. $S(a_1a_2b_3b_4) \neq S(\alpha_1\alpha_2\beta_2\beta_4)$ if $(a_1, a_2) \neq (\alpha_1, \alpha_2)$
5. There are 32 pairs of inputs having a given XOR.
   For each such pair $(\mathbf{a}, \mathbf{b})$ compute $S(\mathbf{a}) \oplus S(\mathbf{b})$
   No more than 8 pairs should yield the same output XOR
6. A criterion similar to 6 but involving 3 S-boxes

6 and 7 are to avoid an attack via differential cryptography (such attacks were introduced in 1990)

The function f is built by compusing two types of functions

1. Expanders
2. S-boxes

The following are simplified examples of each.

1. The following expander expands a 6-bit string to an 8-bit string.

   $$b_1, \ldots, b_6 \mapsto B_1, \ldots, B_8$$

   where

   $$\begin{aligned} B_1 &:= b_1 \\ B_2 &:= b_2 \\ B_3 &:= b_4 \\ B_4 &:= b_3 \\ B_5 &:= b_4 \\ B_6 &:= b_3 \\ B_7 &:= b_5 \\ B_8 &:= b_6 \end{aligned}$$

   Thus, for example $011001 \mapsto 01010101$

2. Two examples of S-boxes

$$S_1: \begin{array}{cccccccc} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{array}$$

$$S_2: \begin{array}{cccccccc} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 010 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{array}$$

An S-box takes as input 4 bits and an output of 3 bits. The first input bit indicates which row of the S-box to use. The next the bits represent a binary number specifying the column. The output is the entry in that row and column.

Note: These S-boxes map from $\{0,1\}^4$ to $\{0,1\}^3$, rather than $\{0,1\}^6 to \{0,1\}^4$, but the idea is the same.

Example 4.14 Consider the string 1010 and suppose we are using the first S-box. The first bit of 1010 is 1, so we use the second row. The next 3 bits are 010, corresponding to the number 2, so we use the second column. Therefore 1010 maps to the entry in row 2 and column 2 of S_1

$$1010 \xrightarrow{S_1} 100$$

An S-box is just a map from $\{0,1\}^n \to \{0,1\}^m$ (chosen to satisfy certain properties).

4.9.5 Key schedule

K is 64 bits (including 8 parity bits). We want to generate $K_1, K_2, \ldots, K_{16}$, each of 48 bits.

We drop the 8 parity bits and apply a fixed permutation $\tau \in \Sigma_{56}$

$$\tau(K) = D_0|E_0 \qquad D_0,E_0 \text{ each of 28 bits}$$

For $1 \le j \le 16$,

$$D_i = \text{Leftshift}_j(D_{i-1})$$
$$E_i = \text{Leftshift}_j(E_{i-1})$$

where Leftshift_j is a left shift of either 1 or 2 places, according to the table

j (Round)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Shift	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Use a fixed projection

$$\underset{i}{\text{proj}} \underbrace{D_i|E_i}_{56 \text{ bits}} \to \underbrace{K_i}_{48 \text{ bits}}$$

For example, $\text{proj}(a_1, \ldots, a_{56}) = (a_{14}, a_{17}, a_{11}, a_{24}, a_1, a_5, \ldots, a_{32})$

It turns out that each bit of K is used in approximately 14 of the 16 rounds. Each bit of c should depend on all the bits of the plaintext. The expansion $E(R)$ is designed so this happens in just a few rounds.

4.9.6 Breaking DES

A few months after DES was released in 1977, Diffie and Hellman proposed building a machine designed to attack DES via a brute force search of the key space (of size 2^{56}). They estimated the machine would cost $20 million (in 1977 dollars)

In 1987 DES underwent its second five year review. The NSA advocated replacing DES with an algorithm whose inner workings only they would know. Eventually DES was recertified in both 1987 and 1992.

In 1993, a Bell-Northern research designed a device that would attack DES efficiently using (fast) telephone switching technology. By 1996, it was also proposed to use a distributed computer using 10s of thousands of machines.

In 1997 RSA Security offered $10,000 for someone to decrypt a DES encrypted message. This was done in 5 months using a distributed computation. 25% of the key space was searched.

In 1998, RSA re-issued the challenge. It was met in 39 days, again using a distributed computation, after searching 85% of the key space.

In the summer of 1998 a special purpose machine "DES Cracker" was built for $200,000.

Des Cracker

Took 2 64-bit blocks of cihpertext. 1500 Chips each containing 24 search units.

Each search unite took a key and used it to decrypet the 1st 64 bit block. If this decryption was interesting (i.e. only a through z, A through Z, 0 through 9, punctuation) the search unite used the same key to decrypt the 2nd 64-bit block.

If both blocks decrypted to interesting text the key is reported back to the control module.

- Probability of 1 byte being interesting is $\frac{69}{256} \approx \frac{1}{4}$
- Probability of 8 bytes=1 block being interesting is $\approx \left(\frac{1}{4}\right) = \frac{1}{65536}$
- Probability of 2 interesting blocks $\approx \left(\frac{1}{65536}\right)^2$

DES cracker took ≈ 4.5 days on average to find the secret key.

Solutions

- Triple DES: $DES_{K_3}(DES_{K_2}(DES_{K_1}(m)))$
- Use 3 keys and apploy
$$DES_{K_2}(K_1 \oplus m) \oplus K_3$$
This scheme is known as DES-X
- E=encrypt in DES, D = decrypt $E_{K_1}(D_{K_2}(E_{K_3}(m)))$ just as good as triple DES. But if $K_2 = K_3$, we get a single DES.