INFORMATION SECURITY

The generic name for the measures that are needed to protect information

COMPUTER SECURITY

The generic name for the collection of tools designed to protect data and to thwart (obstruct/defeat) hackers is Computer Security

NETWORK SECURITY

The generic name for the measures that are needed to protect data during transmission over distributed networks
SECURITY REQUIREMENTS

Security attack:
Any action that compromises the security of information owned by an organization

Security service:
A service that enhances the security of the data processing systems and the transmission of information

Security mechanism:
A mechanism that is designed to detect, prevent or recover from the security attack
(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication

Attack on Availability

Attack on Confidentiality

Attack on Integrity

Attack on Authenticity
Passive Threats

Interception (secrecy)

Release of Message Contents
Traffic Analysis
Active Threats

- Interruption (availability)
- Modification (integrity)
- Fabrication (authenticity)
Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis
Figure 1.1 Model for Network Security
**Trusted Third Party**

- They may be responsible for distributing the secret information to the two principals while keeping it from opponent
- May be needed to arbitrate disputes between the two principals concerning authenticity of a message transmission

**Four Basic Tasks**

- Design an algorithm for performing the security-related transformation
- Generate the secret information to be used with the algorithm
- Develop methods for distribution and sharing of the secret information
- Specify a protocol to be used by the two parties.
Figure 1.2 Network Access Security Model
Human Attack

- A hacker who gets satisfaction from breaking and entering a computer system
- A disgruntled employee who wishes to do damage
- A criminal who seeks to exploit computer assets for financial gain

Software Attack

- Viruses and worms are two examples of software attacks
- They can be inserted into a system across a network
SECURITY MECHANISM

- Needed to cope with unwanted access fall into two broad categories:

  - It might be termed a gatekeeper function – it includes a password based login procedures that are designed to deny access to all but authorized users – screening logic that is designed to detect and reject worms, viruses and other similar attacks
  - Internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders
NONREPUDIATION

- It prevents from either sender or receiver denying a transmitted message.
- Nonrepudiation refers to the protection of communication partners in cases where one of them might claim that data has not been sent or received.
- If this involves a legal dispute, it would be important for the sender of the information to prove that the receiver had received it or for the receiver to prove that the message was sent by the sender.
- Nonrepudiation protects both sender and receiver.
- Different encryption techniques have different levels of success in providing these services.
Figure 2.1  Simplified Model of Symmetric Encryption
Figure 2.2 Model of Symmetric Cryptosystem
Cryptographic systems are generically classified along three independent dimensions:

- The type of operations used for transforming plaintext to ciphertext:
  - Substitution
  - Transposition

- The number of keys used:

  **One Key:**
  - The sender and receiver use the same key
  - The system is referred to as symmetric, single-key, secret-key or conventional encryption

  **Two Keys:**
  - The sender and receiver use different keys.
  - The system is referred to as asymmetric, two-key or public key encryption.
The way in which the plain text is processed:

**Block cipher:**
- Process the input one block of elements at a time
- Producing an output block for each input block

**Stream cipher:**
- Processes the input elements continuously
- Producing output one element at a time, as it goes along
**SUBSTITUTION:**

Example: Substitute every letter in a message with the letter that is three letter further on, when the letter $z$ is reached the cipher comes back to $a$ again.

Plaintext: YOUAREACOMPUTEREXPERT

Ciphertext: BRXDUHDFRPSXWUHASHUW
TRANSPOSITION:

Example: Arrange the message in the column format and reading row by row.

Plaintext: YOUAREACOMPUTEREXPERT

Y E P E T
O A U X
U C T P
A O E E
R M R R

Ciphertext: YEPETOAUXMLPATOEOERMRR
Cryptanalysis

- The process of attempting to discover the plaintext (X) or key (K) or both is known as cryptanalysis.

- Cryptanalysis is possible depending on the nature of the encryption algorithm and the information available.

- If ciphertext is the only one available, it is difficult to carry out cryptanalysis.
ASSUMPTION

- In general, we assume that the opponent knows the algorithm used for encryption.

- Why we assume? If an encryption scheme is developed under this assumption, the scheme is robust to attack.

BRUTE-FORCE APPROACH

- One possible attack under the above assumption is the brute-force approach of trying all possible keys.

- However, if the key space is very large, this becomes impractical.
<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Known to Cryptanalyst</th>
</tr>
</thead>
</table>
| Ciphertext only     | • Encryption algorithm  
                      • Ciphertext to be decoded                                                      |
| Known plaintext     | • Encryption algorithm  
                      • Ciphertext to be decoded  
                      • One or more plaintext-ciphertext pairs formed with the secret key            |
| Chosen plaintext    | • Encryption algorithm  
                      • Ciphertext to be decoded  
                      • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key |
| Chosen ciphertext   | • Encryption algorithm  
                      • Ciphertext to be decoded  
                      • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key |
| Chosen text         | • Encryption algorithm  
                      • Ciphertext to be decoded  
                      • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key  
                      • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key |
Substitution Techniques

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
Caesar Cipher

• earliest known substitution cipher
• by Julius Caesar
• first attested use in military affairs
• replaces each letter by 3rd letter on

example:
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
Caesar Cipher

• can define transformation as:
  a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z 
  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z  A  B  C 

• mathematically give each letter a number
  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 

• then have Caesar cipher as:
  \[ C = E(p) = (p + k) \mod (26) \]
  \[ p = D(C) = (C - k) \mod (26) \]
Cryptanalysis of Caesar Cipher

• only have 26 possible ciphers
  – A maps to A,B,..Z
• could simply try each in turn
• a brute force search
• given ciphertext, just try all shifts of letters
• do need to recognize when have plaintext
• eg. break ciphertext "GCUA VQ DTGCM"
## Possible Keys for Caesar Cipher

| plain cipher | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 1            | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| 2            | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| 3            | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| 4            | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| 5            | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| 7            | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| 8            | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| 9            | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| 10           | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| 12           | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| 13           | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| 14           | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 15           | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 16           | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| 17           | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| 19           | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| 20           | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| 22           | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| 23           | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| 25           | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |
Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long

Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
 Plaintext:  ifwewishtoreplaceletters
 Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
Monoalphabetic Cipher Security

• now have a total of 26! keys
• with so many keys, might think is secure
• but would be !!!WRONG!!!
• problem is language characteristics
Language Redundancy and Cryptanalysis

- human languages are **redundant**
- letters are not equally commonly used
- in English e is by far the most common letter
- then T, R, N, I, O, A, S
- other letters are fairly rare
- cf. Z, J, K, Q, X
- have tables of single, double & triple letter frequencies
Figure 2.5  Relative Frequency of Letters in English Text
Example Cryptanalysis

- **given ciphertext:**
  
  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFAPPDTSVPQUZWYMXUZUHSX
  EPYEPODPDZSZUFPOMBZWPFPUPZHMMDJUDTMOMHQ

- **count relative letter frequencies (see text)**

```
<table>
<thead>
<tr>
<th>Letter</th>
<th>Relative Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>13.33</td>
</tr>
<tr>
<td>Z</td>
<td>11.67</td>
</tr>
<tr>
<td>S</td>
<td>8.33</td>
</tr>
<tr>
<td>U</td>
<td>8.33</td>
</tr>
<tr>
<td>O</td>
<td>7.50</td>
</tr>
<tr>
<td>M</td>
<td>6.67</td>
</tr>
<tr>
<td>H</td>
<td>5.83</td>
</tr>
<tr>
<td>D</td>
<td>5.00</td>
</tr>
<tr>
<td>E</td>
<td>5.00</td>
</tr>
<tr>
<td>V</td>
<td>4.17</td>
</tr>
<tr>
<td>X</td>
<td>4.17</td>
</tr>
<tr>
<td>F</td>
<td>3.33</td>
</tr>
<tr>
<td>W</td>
<td>3.33</td>
</tr>
<tr>
<td>Q</td>
<td>2.50</td>
</tr>
<tr>
<td>T</td>
<td>2.50</td>
</tr>
<tr>
<td>A</td>
<td>1.67</td>
</tr>
<tr>
<td>B</td>
<td>1.67</td>
</tr>
<tr>
<td>G</td>
<td>1.67</td>
</tr>
<tr>
<td>Y</td>
<td>1.67</td>
</tr>
<tr>
<td>I</td>
<td>0.83</td>
</tr>
<tr>
<td>J</td>
<td>0.83</td>
</tr>
<tr>
<td>C</td>
<td>0.00</td>
</tr>
<tr>
<td>K</td>
<td>0.00</td>
</tr>
<tr>
<td>L</td>
<td>0.00</td>
</tr>
<tr>
<td>N</td>
<td>0.00</td>
</tr>
<tr>
<td>R</td>
<td>0.00</td>
</tr>
</tbody>
</table>
```
Example Cryptanalysis

• guess P & Z are e and t

• guess ZW is th and hence ZWP is the

• proceeding with trial and error finally get:

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow
Playfair Cipher

• not even the large number of keys in a monoalphabetic cipher provides security
• one approach to improving security was to encrypt multiple letters
• the Playfair Cipher is an example
• invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair
EXAMPLE

1. Consider a keyword: monnarcchy

2. Construct the matrix by

   - filling in the letters of the keyword (minus duplicates) from left to right and top to bottom

   - filling in the remainder of the matrix with the remaining letters in the alphabetic order.

   - The letters I and J count as one letter.

<table>
<thead>
<tr>
<th>M</th>
<th>O</th>
<th>N</th>
<th>A</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>H</td>
<td>Y</td>
<td>B</td>
<td>D</td>
</tr>
<tr>
<td>E</td>
<td>F</td>
<td>G</td>
<td>I/J</td>
<td>K</td>
</tr>
<tr>
<td>L</td>
<td>P</td>
<td>Q</td>
<td>S</td>
<td>T</td>
</tr>
<tr>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Z</td>
</tr>
</tbody>
</table>
3. Plaintext is encrypted two letters at a time according to the following rules:

- Repeating plaintext letters that would fall in the same pair:
  - Separate with a filler letter.
  - Example: balloon => ba ll oo n => ba lx lo on

- Plaintext that fall in the same row of the matrix:
  - Replace by the letter on the right circularly.
  - Example: ar is encrypted as RM

- Plaintext that fall in the same column of the matrix:
  - Replace by the letter beneath circularly.
  - Example: mu is encrypted as CM

- Otherwise
  - Replace each plaintext by the letter that lies in its own row and the column occupied by the other plaintext letter.
  - Example: “hs” is encrypted as BP and “ea” as IM.
Security of the Playfair Cipher

- security much improved over monoalphabetic
- since have 26 x 26 = 676 digrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- and correspondingly more ciphertext
- was widely used for many years (eg. US & British military in WW1)
- it can be broken, given a few hundred letters
- since still has much of plaintext structure
Hill Cipher

- Developed by the mathematician Lester Hill in 1929.
- It takes $m$ successive plaintext letters and substitutes for the $m$ ciphertext letters.
- It is based on $m \times m$ matrix transformation to obtain linear equations.
- It assigns 0, 1, 2, ... 25 values for a, b, c, ... z.
Consider $m = 3$,

**Encryption:**

\[
\begin{pmatrix}
C_1 \\
C_2 \\
C_3
\end{pmatrix} = \begin{pmatrix}
k_{11} & k_{12} & k_{13} \\
k_{21} & k_{22} & k_{23} \\
k_{31} & k_{32} & k_{33}
\end{pmatrix} \begin{pmatrix}
p_1 \\
p_2 \\
p_3
\end{pmatrix} \mod 26
\]

or simply

\[C = KP, \text{ where } C \text{ is the ciphertext, } P \text{ is the plaintext and } K \text{ is the transform matrix (or encryption key)}\]

**Decryption:**

\[P = K^{-1}C\]
Polyalphabetic Ciphers

• another approach to improving security is to use multiple cipher alphabets
• called polyalphabetic substitution ciphers
• makes cryptanalysis harder with more alphabets to guess and flatter frequency distribution
• use a key to select which alphabet is used for each letter of the message
• use each alphabet in turn
• repeat from start after end of key is reached
Table 2.4 The Modern Vigenere Tableau

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
Vigenère Cipher

• simplest polyalphabetic substitution cipher is the Vigenère Cipher
• effectively multiple caesar ciphers
• key is multiple letters long $K = k_1 \ k_2 \ ... \ k_d$
• $i^{th}$ letter specifies $i^{th}$ alphabet to use
• use each alphabet in turn
• repeat from start after $d$ letters in message
• decryption simply works in reverse
Example

• write the plaintext out
• write the keyword repeated above it
• use each key letter as a caesar cipher key
• encrypt the corresponding plaintext letter
• eg using keyword deceptive

key: deceptive deceptive deceptive deceptive
plaintext: wearediscovered saveyourself
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
Transposition Ciphers

• now consider classical transposition or permutation ciphers
• these hide the message by rearranging the letter order
• without altering the actual letters used
• can recognise these since have the same frequency distribution as the original text
Rail Fence cipher

• write message letters out diagonally over a number of rows
• then read off cipher row by row
• eg. write message out as:
  mematrhhtgpry
  etefetetoeaat

• giving ciphertext
  MEMATRHHTGPRYETEFETEOAAT
Row Transposition Ciphers

- a more complex scheme
- write letters of message out in rows over a specified number of columns
- then reorder the columns according to some key before reading off the rows

Key: 4 3 1 2 5 6 7
Plaintext: a t t a c k p o s t p o n e d u n t i l t w o a m x y z
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
Product Ciphers

• ciphers using substitutions or transpositions are not secure because of language characteristics
• hence consider using several ciphers in succession to make harder, but:
  – two substitutions make a more complex substitution
  – two transpositions make more complex transposition
  – but a substitution followed by a transposition makes a new much harder cipher
• this is bridge from classical to modern ciphers
Rotor Machines

• before modern ciphers, rotor machines were most common product cipher
• were widely used in WW2
  – German Enigma, Allied Hagelin, Japanese Purple
• implemented a very complex, varying substitution cipher
• used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted
• with 3 cylinders have $26^3=17576$ alphabets
Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts