Introduction to Security and Cryptography

Introduction

- Digital Information are now everywhere
- Some information are assets and have high value
- Requires information security mechanisms to secure them.
- The NIST standard FIPS 199 lists the following as security objectives(goals) for information and information systems.
  - Confidentiality
  - Integrity
  - Availability

Security Goals

- **Confidentiality**
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity**
  - Guarding against improper information modification or destruction, with ensuring information nonrepudiation and authenticity.
  - A loss of integrity is the unauthorized modification or destruction of information.
- **Availability**
  - Ensuring timely and reliable access to and use of information.
  - A loss of availability is the disruption of access to information or an information system.

Additional Security Concepts

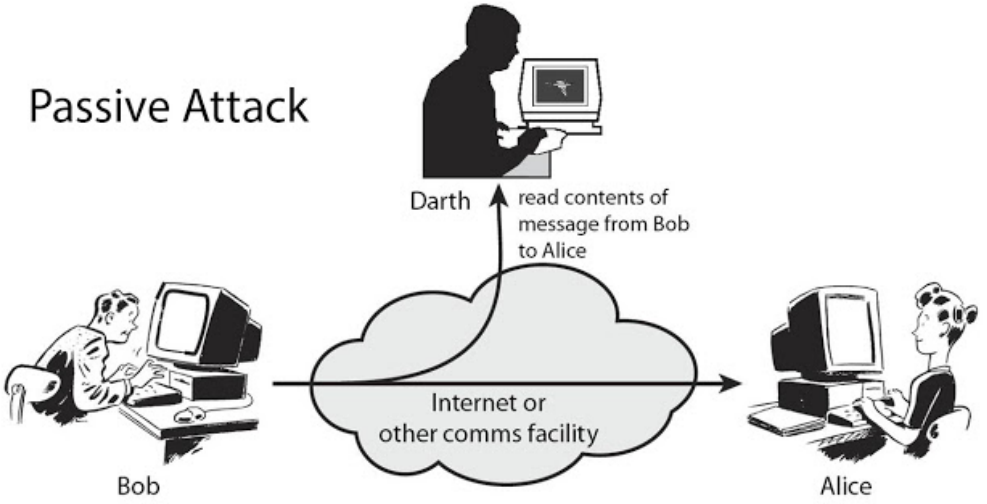
- **Authenticity**
  - The property of being genuine and being able to be verified and trusted
  - Confidence in the validity of a transmission, a message, or message originator
- **Accountability**
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - Supports nonrepudiation, deterrence, and after-action recovery and legal action.
  - Activity records are logged to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

X.800, The Security Architecture for OSI

- **Security attack**: An action that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device) that is designed to detect, prevent, or recover from a security attack.
- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
  - Intended to counter security attacks
  - Make use of one or more security mechanisms to provide the service.

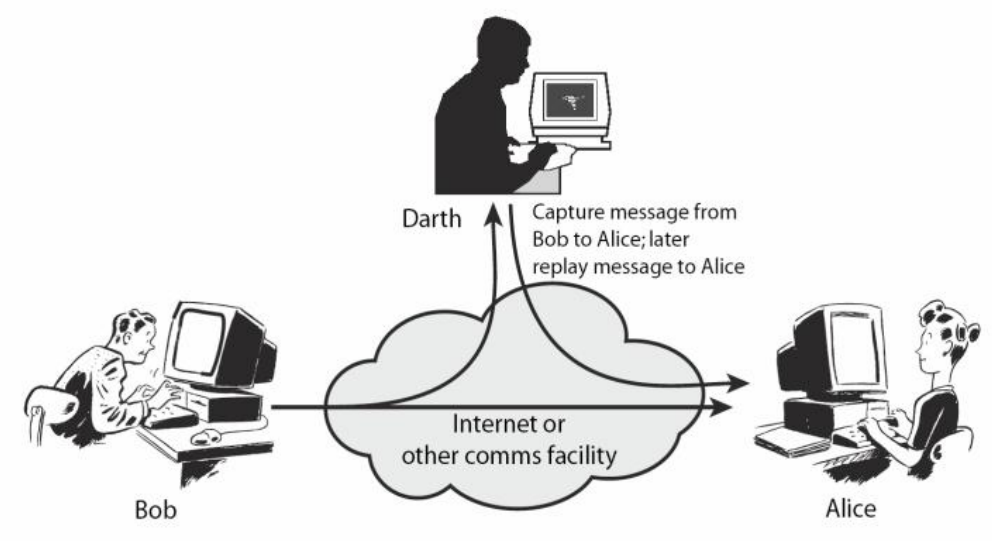
Security Attacks

- **Passive Attacks**
  - in the nature of eavesdropping on, or monitoring
  - obtain information that is being transmitted
  - Two types
    - release of message contents (snooping)
    - traffic analysis.



Security Attacks(2)

- **Active Attacks**
  - involve some modification of the data stream
  - The creation of a false stream
  - Four types
    - Masquerade
    - Replay
    - Modification
    - Denial of service



Active Replay attack

Security Attacks(3)

- Attacks on confidentiality
  - Snooping, Traffic analysis.
- Attacks on Integrity
  - Modification, Masquerading, Replay, Repudiation
- Attack on Availability
  - Denial of Service

Security Services by ITU-T

- Data Confidentiality
  - Confidentiality is the protection of transmitted data from passive attacks.
- Data Integrity
  - Protection of data from modification, insertion, deletion, and replaying by an adversary.
- Authentication
  - Ensuring authentic communication
    - Peer entity authentication
    - Data origin authentication

Security Services by ITU-T (2)

- Access Control
  - Ability to limit and control the access to host systems and applications via communications links
- Nonrepudiation
  - Prevents either sender or receiver from denying a transmitted message
- Availability
  - a system or a resource being accessible and usable upon demand by an authorized entity, according to specifications

Security Mechanisms

- **Encipherment**
  - The use of mathematical algorithms to transform data into a form that is not readily intelligible.
- **Digital Signature**
  - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient to prove the source and integrity of the data unit and protect against forgery.
- **Access Control**
  - Enforce access rights to resources via pin, password, biometrics,etc..
- **Data Integrity**
  - Used to assure the integrity of a data unit or stream of data units.

Security Mechanisms(2)

- **Authentication Exchange**
  - To ensure the identity of an entity by means of information exchange.
- **Traffic Padding**
  - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control**
  - Enables selection of particular physically secure routes for certain data and allows routing changes
- **Notarization**
  - The use of a trusted third party to assure certain properties of a data exchange.

Pervasive Security Mechanisms

- Trusted Functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

Security Mechanism - Services

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Cryptography (Secret writing)

- Study and practice of techniques to store and communicate information in a form (cipher) such that only authorized entities can read and process it.
- Cryptographic Attacks
  - Attacks on cryptographic techniques
- Types of Cryptographic attacks
  - Cryptanalytic Attacks : Combination of statistical and algebraic techniques with the aim to retrieve secret key of ciphers.
  - Non-cryptanalytic Attacks : Does not explore the mathematical aspects of the cryptographic techniques

Stegenography

- Means “covered writing” in greek
- Concealing the message itself by covering with something else.
- Mostly message is hidden inside another data.

Classical Encryption Techniques

Substitution Techniques

- In a substitution technique, the letters of plaintext are replaced by other letters or by numbers or symbols.
- For binary: a sequence of bits in plaintext bit patterns is replaced with ciphertext bit patterns.
- We shall study
  - Caesar Cipher / Additive Cipher
  - Monoalphabetic Cipher
  - Multiplicative Cipher
  - Affine Cipher
  - Playfair Cipher
  - Hill Cipher

Caesar Cipher

- The original Caesar cipher replaces each letter of the alphabet with the letter standing three places further down the alphabet

  plain: 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

  cipher: 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

- If a to z is mapped numerical equivalent from 0 to 25 respectively, then

  Encryption : $C = E(3, p) = (p + 3) \bmod 26$

  Decryption : $p = D(3, C) = (C - 3) \bmod 26$

Additive Cipher/Shift Cipher

- Generic form of Caesar cipher

  Encryption : $C = E(k, p) = (p + k) \bmod 26$

  Decryption : $p = D(k, C) = (C - k) \bmod 26$

  - Where k is the key
- Example:

  Plaintext : “hello”

  Key = 5, then

  Ciphertext = “MJQQT”

Additive Cipher/Shift Cipher Cryptanalysis

- The brute-force attack is easily performed when a ciphertext is known
  - The encryption and decryption algorithms are known.
  - There are only 25 keys to try.
  - The language of the plaintext is known and easily recognizable.

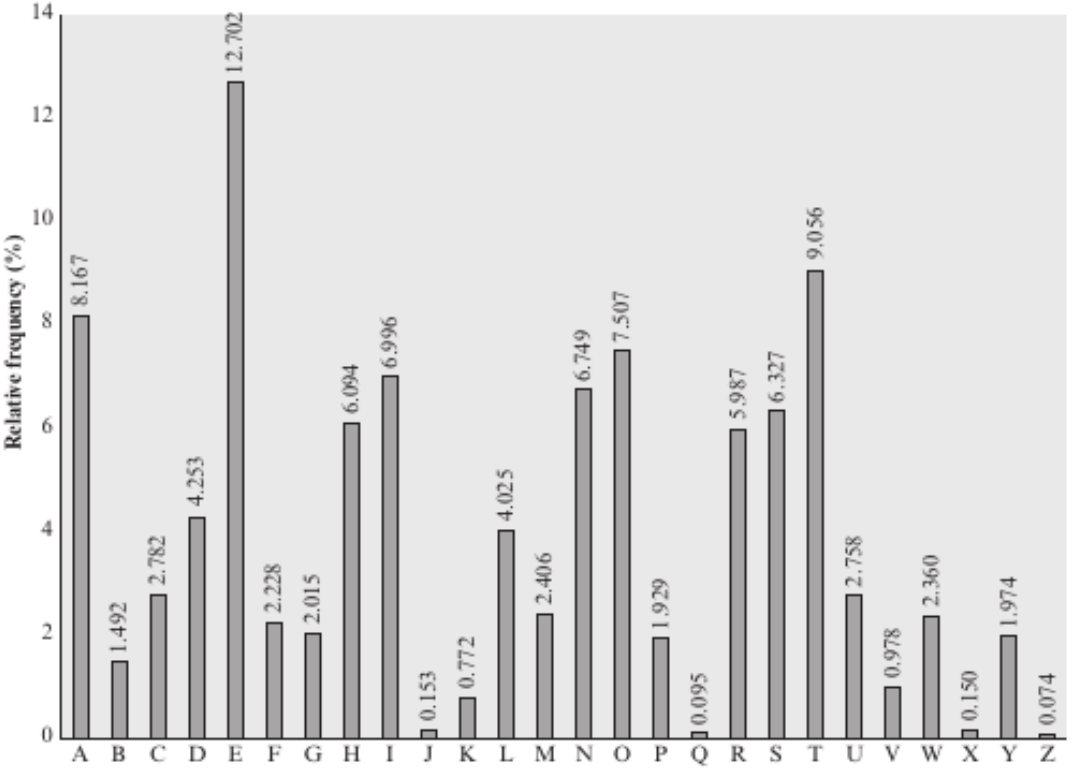
Monoalphabetic Cipher

- The “cipher” line can be any permutation of the 26 alphabetic characters
- Key is 26 letter long
- There are 26! or greater than 4×10^{26} possible keys.

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:  ifwewishtoreplaceletters
Cipher text: WIRFRWAJUHYFTSDVFSFUUFYA
```

Monoalphabetic Cipher Cryptanalysis

- Nature of the text should be known
- Find the relative frequency of the letters
- Compared to a standard frequency distribution for English
- Accurate when message is long



Relative Frequency of Letters in English Text

Monoalphabetic Cipher Cryptanalysis(2)

- A more powerful approach is to look at the frequency of two-letter combinations, known as digrams.
- The most common such digram is “th”
- As per earlier attack, ‘e’ is the most frequently occurring letter. So, using this we can look for pattern of frequent term “the”

Multiplicative Cipher

- Encryption : $C = E(k, p) = (p \times k) \bmod 26$
- Decryption : $p = D(k, C) = (C \times k^{-1}) \bmod 26$
- The plaintext and ciphetext are integers in Z_{26}
- The key is in Z_{26}^{*}, which is the set of all elements with unique multiplicative inverse in modulo 26

Affine Cipher

- Encryption : $C = E(k_1,k_2, p) = ((p \times k_1)+k_2) \bmod 26$
- Decryption : $p = D(k_1,k_2, C) = ((C-k_2) \times k_1^{-1}) \bmod 26$

Plaintext	a	f	f	i	n	e		c	i	p	h	e	r
x	0	5	5	8	13	4		2	8	15	7	4	17
5x+8	8	33	33	48	73	28		18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2		18	22	5	17	2	15
Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P

Ciphertext	I	H	H	W	V	C		S	W	F	R	C	P
y	8	7	7	22	21	2		18	22	5	17	2	15
21(y - 8)	0	-21	-21	294	273	-126		210	294	-63	189	-126	147
21(y - 8) mod 26	0	5	5	8	13	4		2	8	15	7	4	17
Plaintext	a	f	f	i	n	e		c	i	p	h	e	r

Affine Ciphers Cryptanalysis

- Chosen plaintext attack
  - If for a pair of letters the corresponding ciphertext letters are known, then using the affine cipher equation and congruence equations the keys can be predicted.

- Two principal methods are used in substitution ciphers to minimize the survival of the plaintext structures in the ciphertext:
  - Encrypt multiple letters of plaintext
  - Multiple cipher alphabets.

Playfair Cipher

- Use of a 5 × 5 matrix of letters constructed using a keyword
- The matrix is constructed by filling in the letters of the keyword (no duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order.
- For keyword “monarchy” , the matrix is shown here.
- The letters I and J count as one letter.

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

Playfair Cipher(2)

- Encryption/Decryption Rules:
  - Two letters in the same pair are separated with a filler letter, such as x, so that “balloon” would be treated as “ba lx lo on”.
  - Pair of letters that fall in the same row of the matrix are each replaced by the letter to the right, in circular way. For example, ‘ar’ is encrypted as RM.
  - Two letters in the same column are each replaced by the letter beneath, in a circular way. For example, ‘mu’ is encrypted as CM.
  - Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. For example, ‘hs’ becomes BP and ‘ea’ becomes IM (or JM).

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

Playfair Cipher Cryptanalysis

- It leaves much of the structure of the plaintext language intact
- A typical frequency distribution of the 26 alphabetic characters is same for any monoalphabetic substitution cipher
- If we find : no. of occurrences of each letter / no. of occurrences of the most frequently used letter, then it can solve the substitution ciphers.

Hill Cipher

- Here, *m* successive plaintext letters are substituted by *m* ciphertext letters.
- The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, ... , z = 25).
- For *m* = 3, the system can be described as

  $c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$

  $c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$

  $c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$
- Key matrix K must have multiplicative inverse

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

Hill Cipher

For example, the plaintext "code is ready" can make a 3 × 4 matrix when adding extra bogus character "z" to the last block and removing the spaces. The ciphertext is "OHKNIHGKLISS".

$$\overset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} = \overset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} \overset{K}{\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}}$$

a. Encryption

$$\overset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} = \overset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} \overset{K^{-1}}{\begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}}$$

b. Decryption

Hill Cipher Cryptanalysis

- Hill cipher is strong against a ciphertext-only attack
- Easily broken with a known plaintext attack

Polyalphabetic cipher

- A set of related monoalphabetic substitution rules is used.
- A key determines which particular rule is chosen for a given transformation.
- We shall study
  - Vigenère Cipher
  - Vernam Cipher

Vigenère Cipher

- For a sequence of plaintext letters P = $p_0, p_1, p_2, \ldots, p_{n-1}$ and a key consisting of the sequence of letters K = $k_0, k_1, k_2, \ldots, k_{m-1}$, where m < n.
- The sequence of ciphertext letters C = $C_0, C_1, C_2, \ldots, C_{n-1}$ is calculated as follows:

$$
\begin{aligned}
C = C_0, C_1, C_2, \ldots, C_{n-1} &= \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, \ldots, k_{m-1}), (p_0, p_1, p_2, \ldots, p_{n-1})] \\
&= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26, \\
&\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26, \ldots
\end{aligned}
$$

Example: Vigenère Cipher

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenère Cipher Cryptanalysis

- Find the length of the key
  - Kasiski test : looking for repetitive text segment length >3 in ciphertext
- Find the key itself
  - Apply frequency attack to the Kasiski test

Vernam Cipher

- Gilbert Vernam system works on binary data (bits) rather than letters.
- The system can be expressed succinctly as follows:

  $c_i = p_i \oplus k_i$

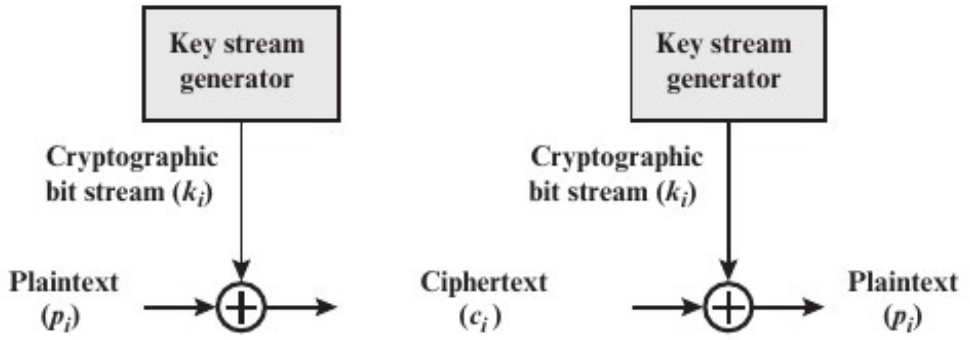
  where

  p_i = ith binary digit of plaintext

  k_i = ith binary digit of key

  c_i = ith binary digit of ciphertext

  $\oplus$ = exclusive-OR (XOR) operation



- Vernam proposed the use of a running loop of tape for construction of the key
- worked with a very long but repeating keyword
- But, it can be broken with sufficient ciphertext,

One time pad

- An improvement to the Vernam cipher that yields the ultimate in security
- Uses a random key that is as long as the message, so that the key need not be repeated
- Each new message requires a new key of the same length as the new message.
- Such a scheme, known as a one-time pad, is unbreakable

Transposition Techniques

- Achieved by performing some sort of permutation on the plaintext letters
- **Rotor machine**