Introduction to Classical Cryptography

- Cryptography is the science or art of secret writing.
- The fundamental objective of cryptography is to enable two people (Alice and Bob) to communicate over an insecure channel in such a way that an opponent (Oscar) cannot understand what is being said.

- Plaintext : the information that Alice wants to send to Bob.
- Alice encrypts the plaintext, using a predetermined key, and send the resulting ciphertext to Bob over the public channel.
- Upon receiving the ciphertext
  - Oscar cannot determine what the plaintext was
  - But Bob knows the encryption key, can decrypt the ciphertext and get the plaintext.

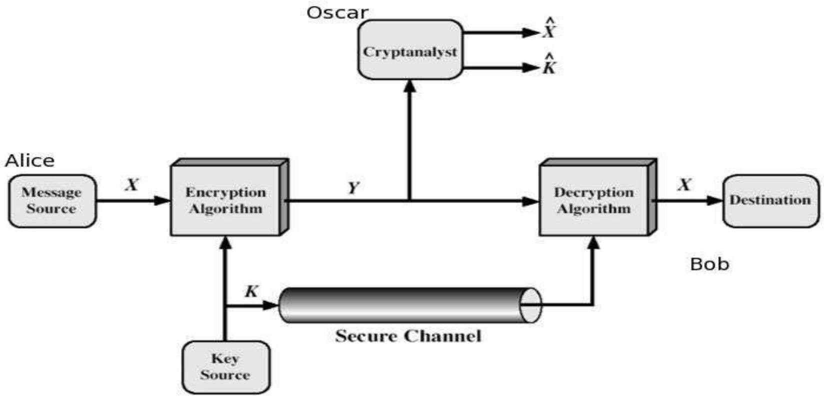


Figure 1: Communication Channel.

Conventional Encryption

- Also termed single-key or symmetric encryption

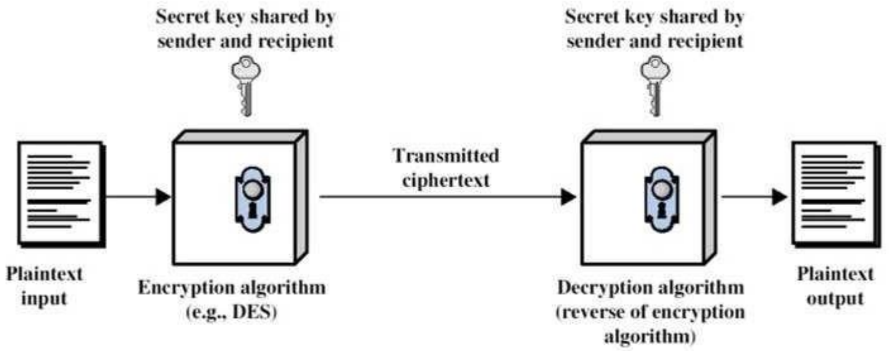

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2: Simplified model of conventional encryption.

Cryptosystem

- Cryptosystem is a five tuple (P, C, K, E, D)
  - Plaintext Space (P): set of all possible plaintexts
  - Cipherext Space (C): set of all possible ciphertexts
  - Key Space (K): set of all possible keys
  - E: set of all possible encryption rules and D: set of all possible decryption rules
- For each $k \in K$, there is an encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$ such that $d_k(e_k(x)) = x$ for every plaintext $x \in P$

- A practical cryptosystem should satisfy
  - Each encryption function e_k and each decryption function d_k should be efficiently computable.
  - An opponent, upon seeing the ciphertext string y, should be unable to determine the key k that was used, or the plaintext string x

- The process of attempting to compute the key k, given a string of ciphertext y, is called cryptanalysis.
  - If opponent can determine k, then he can decrypt y just as Bob would, using d_k.
  - Determining k should be as difficult as determining the plaintext string x, given the ciphertext string y.

Shift Cipher

- $Z_{26} = \{0, 1, 2 \ldots, 24, 25\}$
- $\mathrm{P} = \mathrm{C} = \mathrm{K} = Z_{26}$
- For $k \in \mathrm{K}$,

  $e_k(x) = (x + k) \bmod 26$ for $x \in \mathrm{P}$

  $d_k(y) = (y - k) \bmod 26$ for $y \in \mathrm{C}$
- Caesar Cipher is a particular case (for $k = 3$)

Example

- Plaintext is ordinary English text
- Correspondence between alphabetic characters and integer: $A = 0, B = 1, . . . , Y = 24, Z = 25.$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

Encryption

- key *k* = 11
- Plaintext is “wewillmeetatmidnight”
- corresponding sequence of integers:

  22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

- we add 11 (key) to each value (reducing modulo 26):

  7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

- convert the sequence of integers to alphabetic characters:

  Ciphertext is “HPHTWWXPPELEXTOYTRSE”

Decryption

- ciphertext : “HPHTWWXPPELEXTOYTRSE”.
- convert the ciphertext to sequence of integers:

  7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4.

- subtract 11 from each value (reducing modulo 26):

  22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19.

- convert the sequence of integers to alphabetic characters:

  Plaintext is “wewillmeetatmidnight”

Caesar Cipher

- Caesar Cipher is the earliest known (and the simplest). It involves replacing each letter of the alphabet with the letter standing three places further down. This is then wrapped around on itself when the end is reached. For example:

Key:	k=3
Plaintext:	meetmeaftertheparty
Ciphertext:	PHHWPHDIWHUWKHSDUWB

Shift Cipher is not Secure

- Brute-force cryptanalysis easily performed on the shift cipher by trying all 25 possible keys.
- Given a ciphertext string, Oscar successively try the decryption process with $k = 0, 1, 2,$ etc. until get a meaningful text.

- Ciphertext : JBCRCLQRWCRVNBJENBWRWN

$k = 0 \rightarrow$ jbcrclqrwcrvnbjenbwrwn

$k = 1 \rightarrow$ iabqbkpqvbqumaidmavqvm

$k = 2 \rightarrow$ hzapajopuaptlzhclzupul

$k = 3 \rightarrow$ gyzozinotzoskygbkytotk

$k = 4 \rightarrow$ fxynyhmnsynrjxfajxsnsj

$k = 5 \rightarrow$ ewxmxglmrxmqiweziwrmri

$k = 6 \rightarrow$ dvwlwfklqwlphvdyhvqlqh

$k = 7 \rightarrow$ cuvkvejkpvkojucxjupkpg

$k = 8 \rightarrow$ btujudijoujnftbwftojof

$k = 9 \rightarrow$ astitchintimesavesnine

- The key is $k = 9$

Substitution Cipher

- P = C = set of 26-letter English alphabet

  P = $\{a, b, c, \ldots, y, z\}$

  C = $\{A, B, C, \ldots, Y, Z\}$

- K = set of all possible permutations of 26 alphabetic characters.

- For each permutation $\varphi \in$ K,

  $e_\varphi(x) = \varphi(x)$ for $x \in$ P

  $d_\varphi(y) = \varphi^{-1}(y)$ for $y \in$ C, where φ^{-1} is the inverse permutation of φ.

Example

- Encryption function is the permutation φ :

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

- Decryption function is the inverse permutation φ^{-1}:

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	l	r	y	v	o	h	e	z	x	w	p	t	b	g	f	j	q	n	m	u	s	k	a	c	i

- Key: $k = \varphi$
- Ciphertext: MGZVYZLGHCMHJMYXSNHAHYCDLMHA
- Find the plaintext???

- Monoalphabetic Cipher: Each alphabetic character is mapped to a unique alphabetic character
- We use arbitrary monoalphabetic substitution, so there are 26! or $4 \times 10^{26} \approx 2^{88}$ possible permutations, which is a very large number. Thus brute force is infeasible.
- However we will see later that a Substitution Cipher is insecure against frequency analysis.

Vigen`ere Cipher

- Polyalphabetic cipher: use different monoalphabetic substitutions while moving through the plaintext.
- Let m be a positive integer
- $\mathrm{P} = \mathrm{C} = \mathrm{K} = (Z_{26})^m$
- For $k = (k_1, k_2, \ldots, k_m) \in \mathrm{K}$,

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$
$$d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m)$$

- All above operations are performed in Z_{26}

Example

- Correspondence between alphabetic characters and integer: $A = 0, B = 1, \ldots, Y = 24, Z = 25$.
- $m = 6$.
- Keyword is “CIPHER”, this corresponds to the numerical equivalent $k = (2, 8, 15, 7, 4, 17)$

- Plaintext : “thiscryptosystemisnotsecure”.
- Encryption: add modulo 26

19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7
21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19

8	18	13	14	19	18	4	2	20	17	4
4	17	2	8	15	7	4	17	2	8	15
12	9	15	22	8	25	8	19	22	25	19

- Ciphertext:
“V P X Z G I A X I V W P U B T T M J P W I Z I T W Z T ”.

- Transposition techniques: So far all the ciphers we have looked at involved only substitution. A very different kind of mapping is achieved using transposition.

- In its simplest form, the rail fence technique involves writing down the plaintext as a sequence of columns and the ciphertext is read off as a sequence of rows. For example, if we use a rail fence of depth 2 with the plaintext *meet me after the party is over* we get:

m	e	m	a	t	r	h	p	r	y	s	v	r
e	t	e	f	e	t	e	a	t	i	o	e	

- Ciphertext is *mematrhprysvretefeteatioe* which is simply the first row concatenated with the second.

Transposition/Permutation Cipher

- Let m be a positive integer
- P $=$ C $= (Z_{26})^m$
- K $=$ set of all possible permutations of $\{1, 2, \ldots, m\}$
- For each permutation $\pi \in$ K,

$$e_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})$$

$$d_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)})$$

- π^{-1} being the inverse permutation of π

Example

- $m = 6$.
- key is the following permutation π:

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

- inverse permutation π^{-1}:

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

- Plaintext : “defendthehilltopatsunset”

- partition the plaintext into group of six letters:

  defend | thehil | ltopat | sunset

- rearrange according to π:

  fnddee | eitlhh | oaltpt | nestsu

- Ciphertext: "FNDDEEEITLHHOALTPTNESTSU"
- Decryption can be done using π^{-1}

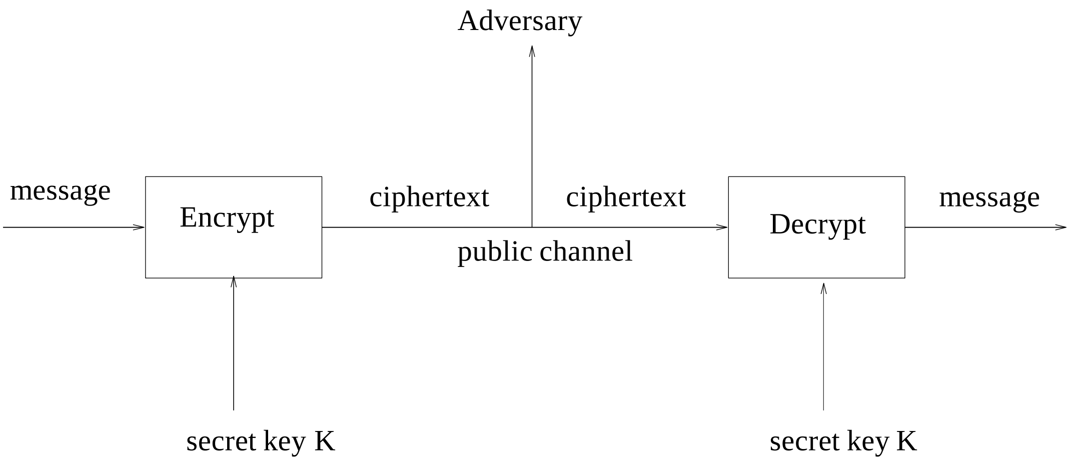
Cryptanalysis

- Brute-force cryptanalysis easily performed on the Shift cipher by trying all 25 possible keys.
- Three characteristics of the problem facilitate the successful use of the brute force approach:

  1. The encryption scheme is known.
  2. There are only a limited no. of keys.
  3. The plaintext is easily recognisable.

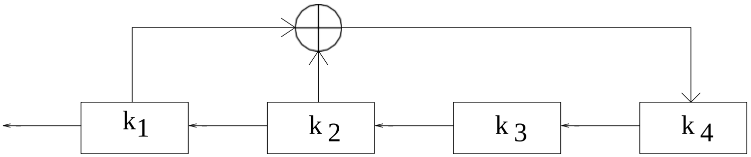
- Most cases, key size tends to be the main problem for brute-force attacks.

Symmetric Key Encryption



- Block ciphers and stream ciphers are two types of symmetric key cryptosystems

Linear Feedback Shift Register (LFSR)



- An LFSR of length m consists of m stages numbered $1, 2, \ldots, m$, each storing one bit and having one input and one output; together with a clock which controls the movement of data.
- The vector $(k_1, k_2, \cdots, k_m)$ would be used to initialize the shift register

- During each unit of time the following operations would be performed concurrently

  (i) k_1 would be tapped as the next keystream bit

  (ii) $k_2, \cdots, k_m$ would each be shifted one stage to the left

  (iii) the “new” value of k_m would be computed to be

$$\sum_{j=1}^{m-1} c_j k_{j+1}$$

  the linear feedback is carried out by tapping certain stages of the register (as specified by the constants c_j having the value “1”) and computing a sum modulo 2 (which is an exclusive-or).

Cryptographic Security

- Kerckhoff's Principle: Assume that the adversary knows the algorithm that is used. The secret is *only* the secret key.
- Attack Models:
  - Ciphertext only attack: The opponent possesses a string of ciphertext, *y*
  - Known plaintext attack: The opponent possesses a string of plaintext, *x*, and the corresponding ciphertext, *y*

- – Chosen plaintext attack: The opponent has obtained temporary access to the encryption machinery. Hence he can choose a plaintext string, x, and construct the corresponding ciphertext string, y.
- – Chosen ciphertext attack: The opponent has obtained temporary access to the decryption machinery. Hence he can choose a ciphertext string, y, and construct the corresponding plaintext string, x.

- Adversarial Goal:
  - Key recovery.
  - Distinguishing attack.
  - Malleability.
  - Other application specific security goals.

Hill Cipher:

The **Hill cipher** is a polygraphic substitution cipher based on linear algebra. developed by the mathematician **Lester S. Hill.** It was the first polygraphic cipher in which it was practical to operate on more than three symbols at once.

Encryption:

C = K P mod 26 ………….(15).

Decryption:

P = K^(-1)C mod 26 ………..(16).

like the other