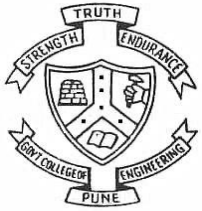
Cryptography and Network Security

Session 4

V. K. Pachghare



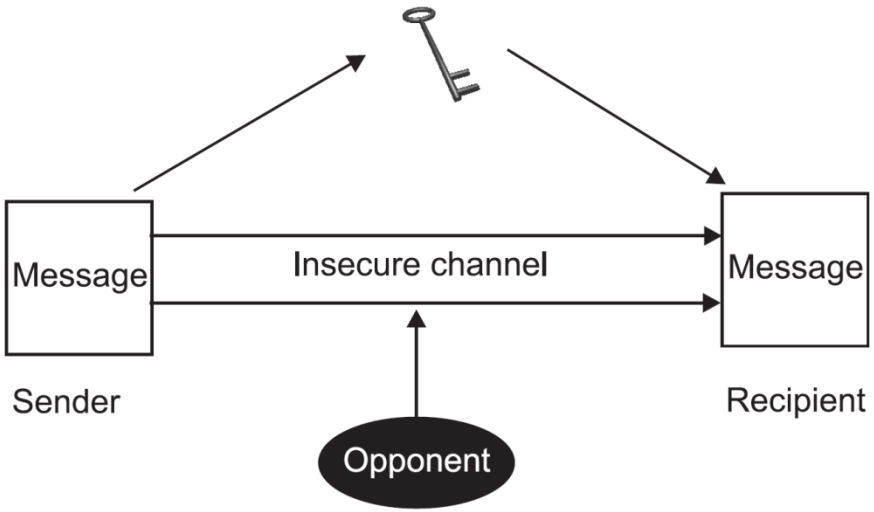
Classical Encryption Techniques

Classical Encryption Techniques

- **Symmetric Encryption**
- **Asymmetric Encryption**

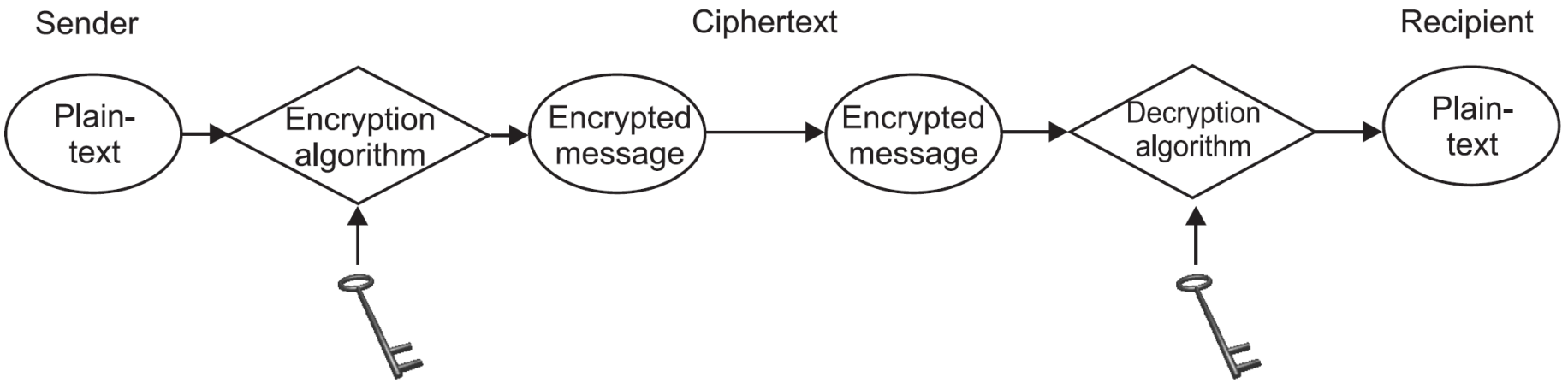
Symmetric Encryption

- Conventional / private-key / single-key
- Sender and recipient share a common key
- Same key is used for encryption and decryption
- DES, Triple DES, AES, IDEA, Blowfish, RC4, RC5, RC6


Message
Insecure channel
Message
Sender
Recipient
Opponent

Components of Symmetric Encryption

- Plaintext
- Encryption Algorithm
- Key
- Ciphertext
- Decryption Algorithm


Sender
Ciphertext
Recipient
Plain-text
Encryption algorithm
Encrypted message
Encrypted message
Decryption algorithm
Plain-text

Asymmetric Encryption

- Two different keys are required: public key and private key
- These keys are mathematically related to each other
- The key which is publically available for all are called public key
- The key which is known only to the owner of the key is called private key
- Diffie-Hellman, RSA, Elliptic Curve Cryptography

Brute Force Attack

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext
- Ex. If key is binary and key size is 12 bits then 2^{12} number of possible attempts are required using Brute Force search

Classical Substitution Ciphers

- Letters of plaintext are replaced by other letters or by numbers or symbols
- Or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- Earliest known substitution cipher by Julius Caesar
- Replaces each letter by 3rd letter
- example:

PT	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
CT	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

– meet me after the toga party

– PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

- Assign each letter to an index starting from 0.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Compute the following.

  (plain letter index + key) mod (total number of letters)
- This will give the index of the encrypted letter.
- The modulus is the total number of letters in the alphabet. For English, this modulus is 26.

- Let's say we have a 5 letter alphabet with only the letters A-E
- First, we assign each letter an index, starting from 0.

A	B	C	D	E
0	1	2	3	4

- We then have to choose a key. Suppose Key is 2.
- Suppose the plaintext is **BEAD**.
- The index of the letter B is 1. So, (1 + 2) mod 5
- = 3 mod 5 = 3
- Corresponding letter for 3 is D.
- Using algorithm on each letter, can you encode the full word as

DBCA

Decryption

(cipher letter index – key + total number of letters) mod (total number of letters)

Ciphertext is **DBCA**

A	B	C	D	E
0	1	2	3	4

Corresponding number for D is 3 and key is 2

PT = (3-2) mod 5 = 1 mod 5 = 1 => B

B=> (1-2) mod 5 = -1 mod 5 = 4 => E

C => (2-2) mod 5 = 0 mod 5 = 0 => A

A => (0-2) mod 5 = -2 mod 5 = 3 => D

PT = **BEAD**

- ***Advantages***
  - This cipher (encryption algorithm) is easy to implement.
- ***Disadvantages***
  - Brute force attack is easily possible.
  - Its observable pattern helps the attacker to find out plaintext easily.
  - Maximum number of keyspace (total number of keys) are 25 which can be easily found out

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: **a**bc**de**fghijklmnopqrstuvwxyz

Cipher: DKV**QF**IBJWPESCXHTMYAUOLRGZN

Plaintext: **BEAD**

Ciphertext: **KFDQ**

Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 10^{26} keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

Cryptanalysis

- Cryptanalysis is the art of breaking codes and ciphers
- a more systematic approach for cryptanalysis is to calculate the frequency distribution of the letters in the cipher text
- This consists of counting how many times each letter appears
- Natural English text has a very distinct distribution that can be used help crack codes

English Letter Frequencies