INFORMATION SECURITY (CA724)

Dr. Ghanshyam S. Bopche
Assistant Professor
Dept. of Computer Applications

February 3, 2022

Assets, Vulnerabilities, Threats, and Adversaries

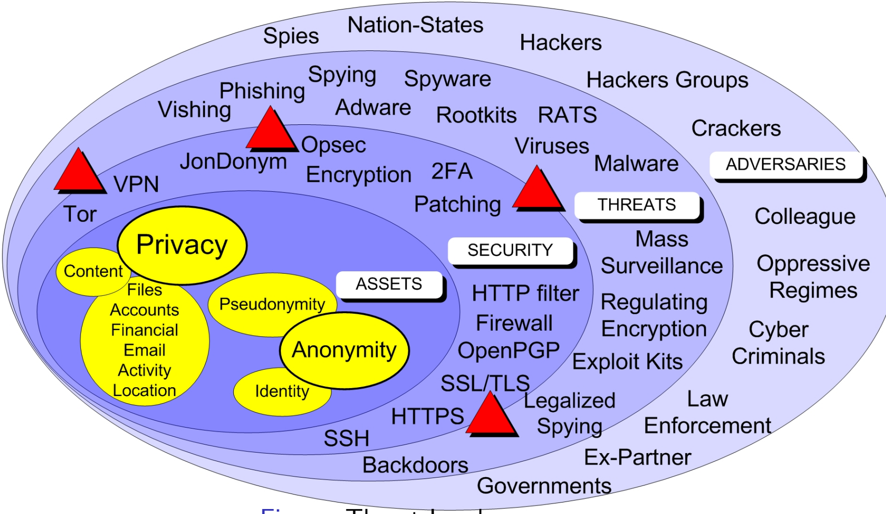


Figure: Threat Landscape

SYLLABUS

- Implementation of Classical Encryption Algorithms
- Implementation of symmetric and public key encryption algorithms.
- Implementation of Hashing algorithms and study of their applications.
- Implementation of authentication algorithms.
- Implementation of Digital Signature using available standards.
- Simulation of various network security issues.
- Simulation of various application security issues.
- Study of well-known vulnerabilities and threats.

Information Security

Protection of data or information

- at rest
- in transit

Security Attributes

- **Confidentiality**
  - The property of non-public information remaining accessible only to authorized parties, whether stored (at rest) or in transit (in motion).
  - Asset should not be disclosed to unauthorized individuals, entities, and processes.
  - Achieved by means of data encryption (use of keyed cryptographic algorithms).
- **Integrity**
  - The property of data, software or hardware remaining unaltered, except by authorized parties.
  - Maintaining the accuracy and completeness of the asset over its entire life-cycle.
  - Achieved by means of error detection and error correction codes (use of cryptographic checksum).

Security Attributes (cont.)

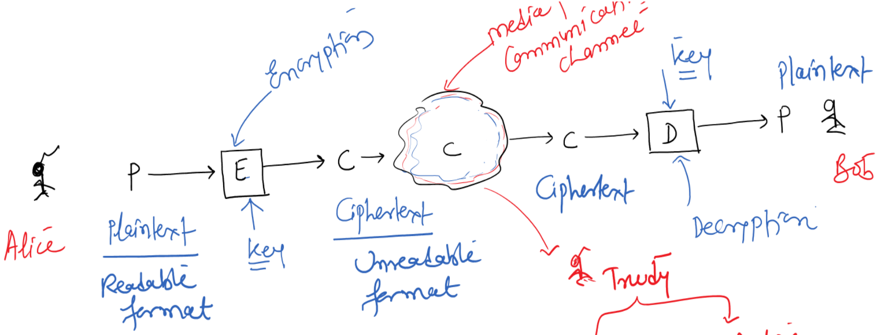
- **Availability**
  - The property of information, services and computing resources remaining accessible for authorized use.
  - Requires protection from intentional deletion and disruption, including denial of service attacks aiming to overwhelm resources.
- **Authentication**
  - Assurance that a principal (users, communicating entities, or system processes), data, or software is genuine relative to expectations arising from appearances or context.
  - Entity authentication: provides assurances that the identity of a principal involved in a transaction is as asserted.
  - Data origin authentication: provides assurances that the source of data or software is as asserted.

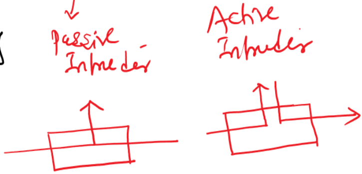
Cryptology

Cryptology = Cryptography + Cryptnalysis

- Cryptography: Devising Cipher
- Cryptnalysis: Breaking Cipher

Traditional Model of Cryptography





Communication Partner : {Alice, Bob}

Intruder : {Trudy}

Classical Excryption Algorithms

1. Caesar Cipher (K-shift method)
2. Double Transposition Cipher
3. Monoalphabetic substitutional algorithm (use of mapping table)
4. Polyalphabetic substitutional algorithm (E.g. Vigenere Cipher)

1) Caesar Cipher

Caesar Cipher
(Substitution Cipher)

Plaintext = B A D $\quad \boxed{k=3}$

Ciphertext = E D G

$$E(x) = y = (x+k) \% 26$$

$$D(y) = x = (x-k) \% 26$$

ⓐ Alphabets Σ:

0	1	2	3		24	25
A	B	C	D	. . . .	Y	Z

ⓑ key = k = 0 − 25

ⓒ plaintext = MONOGRAM

2) Double Transposition Cipher

Double Transposition Cipher
↳ permute the rows and columns of plaintext matrix according to specified permutations.

Plaintext : attackatdawn matrix size $= 3 \times 4$

matrix

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix}$$

Encryption

→ Row permutation $(1,2,3) \longrightarrow (3,2,1)$

→ Column permutation $(1,2,3,4) \longrightarrow (4,2,1,3)$

Decryption

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ d & a & w & n \end{bmatrix} \longrightarrow \begin{bmatrix} d & a & w & n \\ c & k & a & t \\ a & t & t & a \end{bmatrix} \longrightarrow \begin{bmatrix} n & a & d & w \\ t & k & c & a \\ a & t & a & t \end{bmatrix}$$

3×4

Plaintext matrix   Row permutation   Column permutation

$\boxed{\text{Ciphertext} = \text{nadwtkcaata}}$

2) Double Transposition Cipher (cont.)

Decryption

Ciphertext = nadwtkcaatat

matrix size = 3×4

$$\begin{array}{c} \begin{array}{cccc} 4 & 2 & 1 & 3 \end{array} \\ \begin{bmatrix} n & a & d & w \\ t & k & c & a \\ a & t & a & t \end{bmatrix}_{3 \times 4} \end{array}$$

Column permutation $(4,2,1,3) \longrightarrow (1,2,3,4)$

Row permutation $(3,2,1) \longrightarrow (1,2,3)$

3) Monoalphabetic substitutional algorithm

Monoalphabetic Substitutional Algorithm
(use of mapping table)

Mapping Table

A	S
B	U
L	R
D	A
E	N

plaintext = BAD

Ciphertext = U S A

What if plaintext characters repeated?

4) Polyalphabetic substitutional algorithm

Goal: Even though plaintext characters are repeated, the ciphertext characters should not be repeated.
Hence, the concept of key is introduced, for the first time in the world of information/network security.

4) Polyalphabetic substitutional algorithm (cont.)

Vigenere Cipher

key: MEGABUCK

key (column) : ME GAB UCKMEGABUC KME

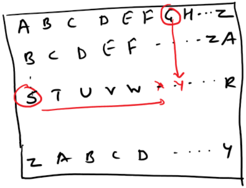
plaintext (row) : WE ARE DISCUSSING NWS

Ciphertext : ... Y S ... W

key (column)

Sender

plaintext (row)



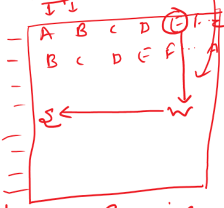
Ciphertext

C, key

Search for W

Receiver

key



plaintext Receiver

Problems based on Caesar Cipher

1. Given that Caesar's cipher is used, find the plaintext from the following ciphertext:
   VSRQJHEREVTXDUSHDQWU
2. Find the plaintext and the key from the ciphertext *CSYEVIXIVQMREXIH* given that the cipher is a simple substitution of the shift-by-n variety.

5) Transpositional Cipher

Goal: Position is required to be disturbed.
Key: MEGABUCK
Plaintext Message: WE ARE DISCUSSING NWS IN ROOM NO # 410

5) Transpositional Cipher (cont.)

Encryption

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
W	E	A	R	E	D	I	S
C	U	S	S	I	N	G	N
W	S	I	N	R	O	O	M
N	O	#	4	1	0	-	-

Decryption

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
W	E	A	R	E	D	I	S
C	U	S	S	I	N	G	N
W	S	I	N	R	O	O	M
N	O	#	4	1	0	-	-

Ciphertext: RSN4 EIR1 IGOEUSO
ASI#SNMWCWNDNOO

Key size) Received ciphertext characters (no. of full rows

last row: leftover

$$8\overline{)30}(3$$
$$\underline{24}$$
$$6$$

6) One-time Pad

Letter	e	h	i	k	l	r	s	t
Binary	000	001	010	011	100	101	110	111

Plaintext: heilhitler

Bit string: 001 000 010 100 001 010 111 100 000 101

Sender Encryption

Ex-OR operation ⊕

Onetime Pad: 111 101 110 101 111 100 000 101 110 000

110 101 100 001 110 110 111 001 110 101

→ s r l h s s t h s r

Ciphertext

110 101 100 001 110 110 111 001 110 101

Ex-OR operation ⊕

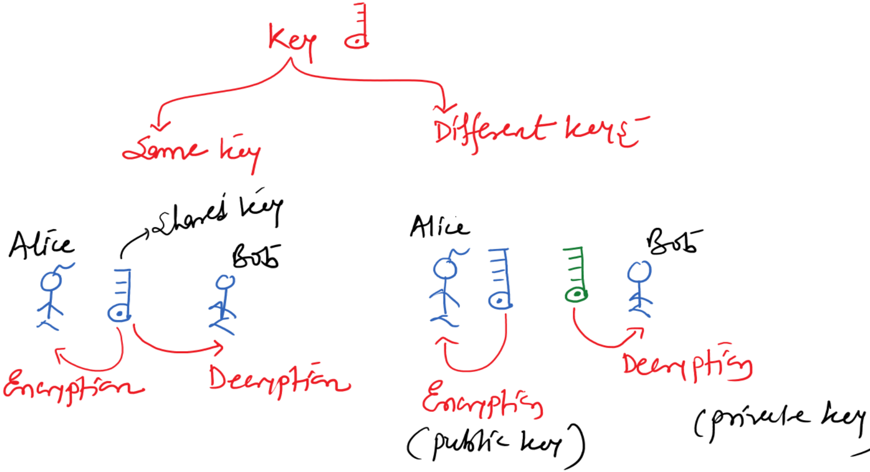
One-time Pad: 111 101 110 101 111 100 000 101 110 000

001 000 010 100 001 010 111 100 000 101

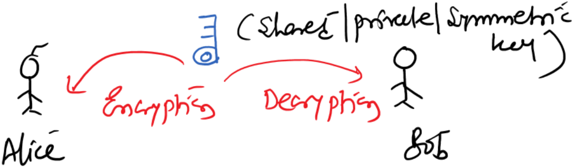
Receiver Decryption

Plaintext → h e i l h i t l e r

Symmetric vs Non-symmetric Key Crypto



Symmetric Key Cryptosystem



Algorithms : ① DES (56 bit key)
② Triple DES (112 or 168 bit key)
③ IDEA (128 bit key)
④ AES (128, 192, ..., bit key)

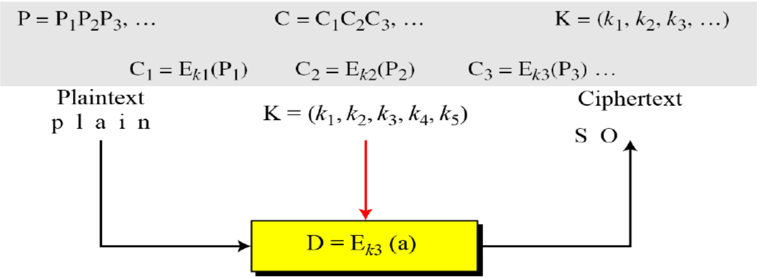
Advantage : Speed ↑

Disadvantage : key distribution

Symmetric Key Cryptosystem (cont.)

Types of Symmetric Encryption

- **Stream Cipher**: a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

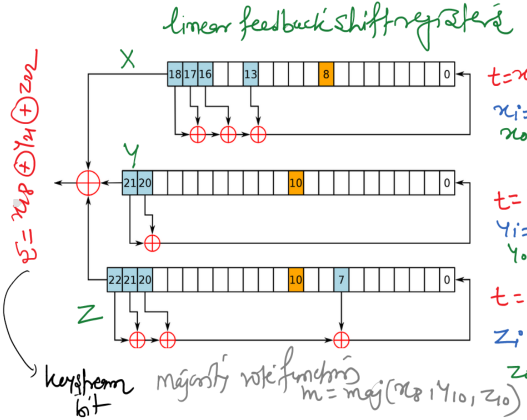


Examples: A5/1 (used by GSM/3G Cell Phones, hardware implementation), RC4 (software implementation), etc.

Symmetric Key Cryptosystem (cont.)

A5/1 Algorithm

Useful Links: A5/1 Algorithm, A5/1 Encryption Algorithm



Register steps:

$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$

$x_i = x_{i-1}$ for $i = 18, 17, 16, \dots, 1$

$x_0 = t$

$\boxed{x_8 == m}$

$t = y_{20} \oplus y_{21}$

$y_i = y_{i-1}$ for $i = 21, 20, 19, \dots, 1$

$y_0 = t$

$\boxed{y_{10} == m}$

$t = z_{20} \oplus z_{21} \oplus z_{22}$

$z_i = z_{i-1}$ for $i = 22, 21, 20, \dots$

$z_0 = t$

$\boxed{z_{10} == m}$

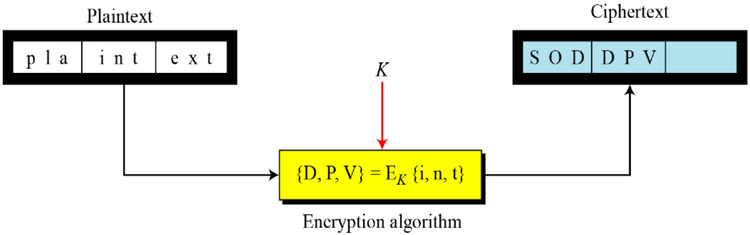
Symmetric Key Cryptosystem (cont.)

RC4

- RC4 produces keystream byte at each step.
- Uses a lookup table containing a permutation of the 256-byte values (self-modifying lookup table).
- **Applications**: SSL, WEP, WPA, etc.
- **Important Liks**: RC4 Basics, RC4 Encryption Algorithm, Attack on RC4.

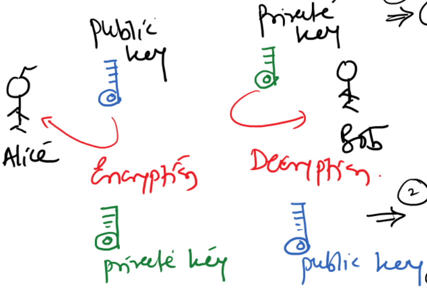
Symmetric Key Cryptosystem (cont.)

- **Block Cipher**: a cryptographic key and algorithm are applied to blocks of data rather than individual bits in a stream.



Examples: DES, 3DES, AES, etc.

Public/Assymetric Key Cryptosystem



① → Confidentiality

② → Digital signature

③ → authentication

④ → Key management (key distribution)

Algorithms: ① RSA
② Knapsack
③ ECC

Disadvantage: Slow (Speed ↓)