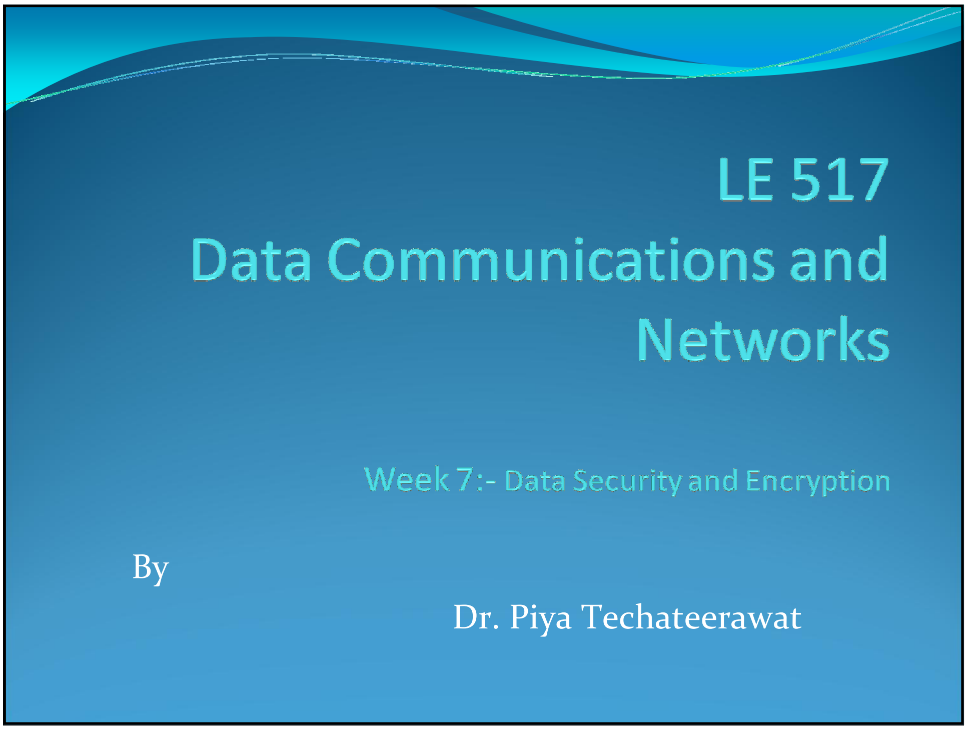
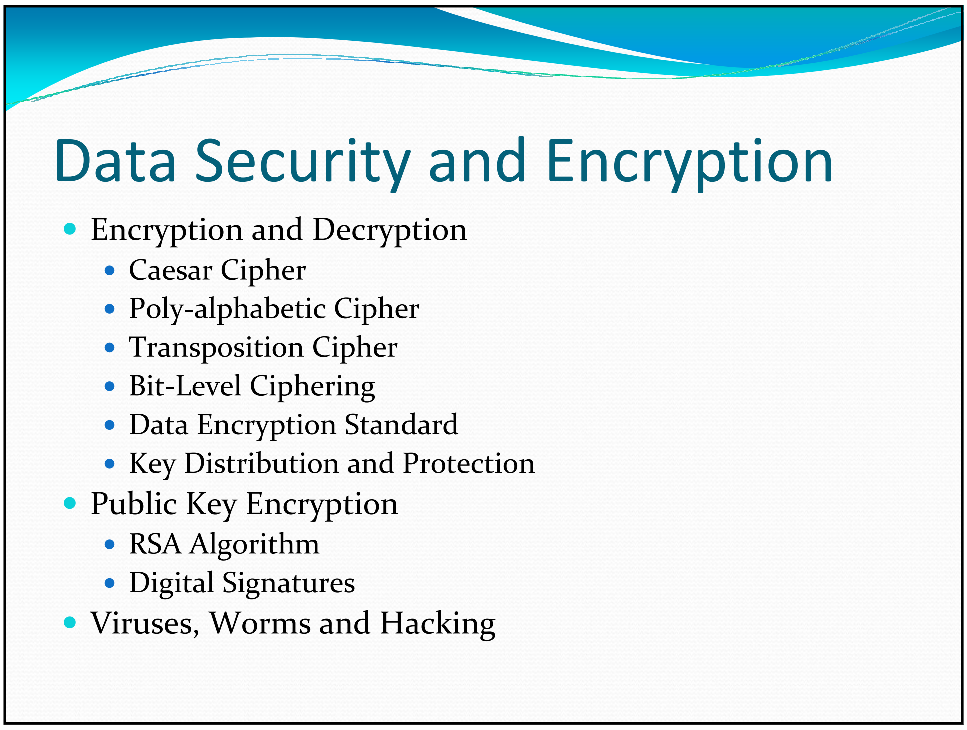


LE 517
Data Communications and Networks

Week 7:- Data Security and Encryption

By

Dr. Piya Techateerawat



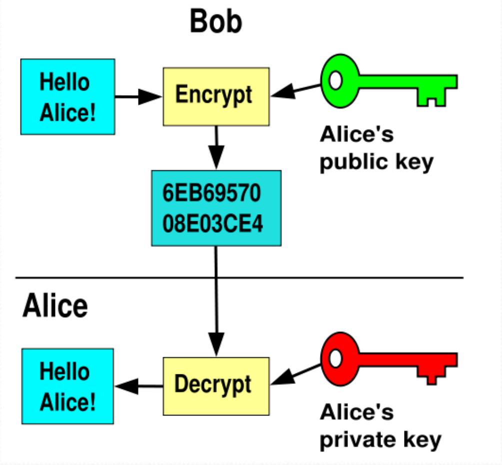
Data Security and Encryption

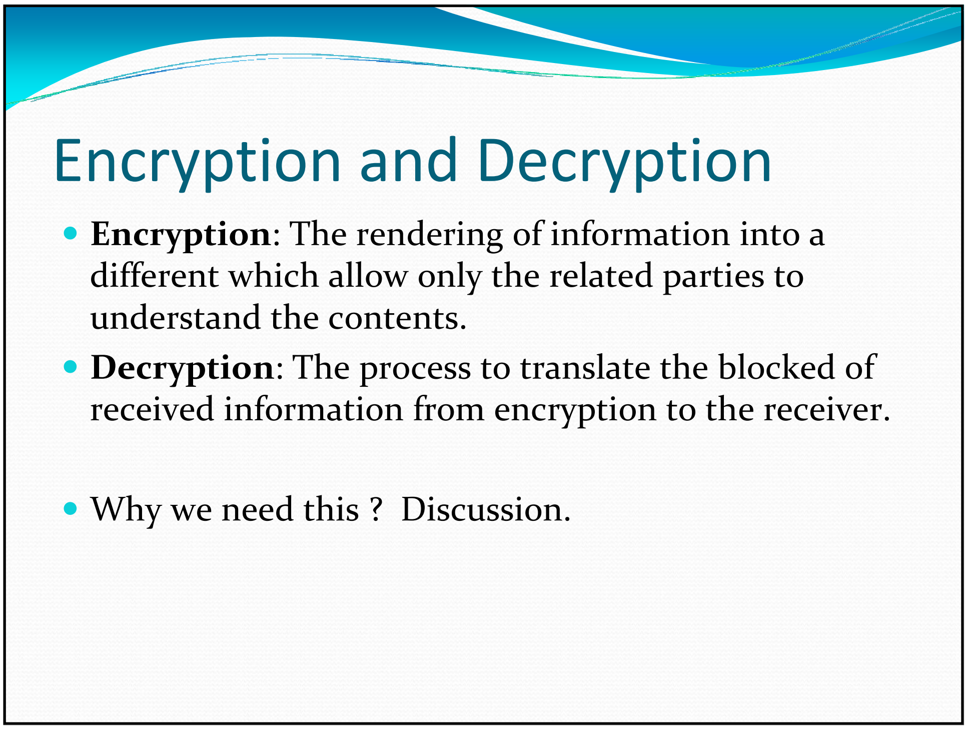
- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking

Data Security and Encryption

- **Encryption and Decryption**
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking

Encryption and Decryption

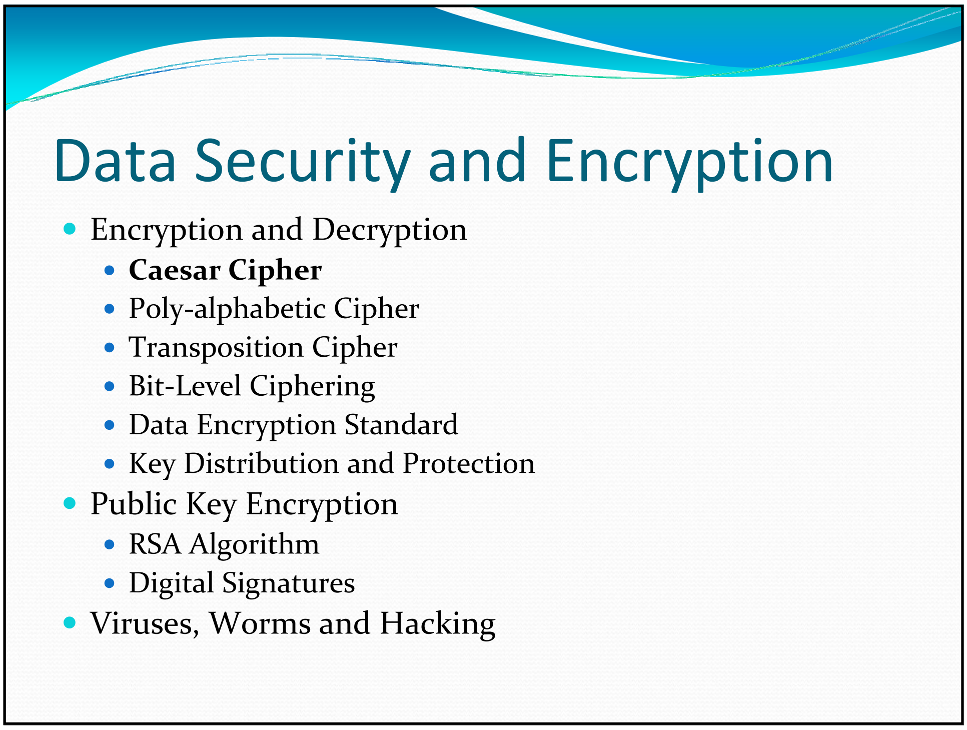




Encryption and Decryption

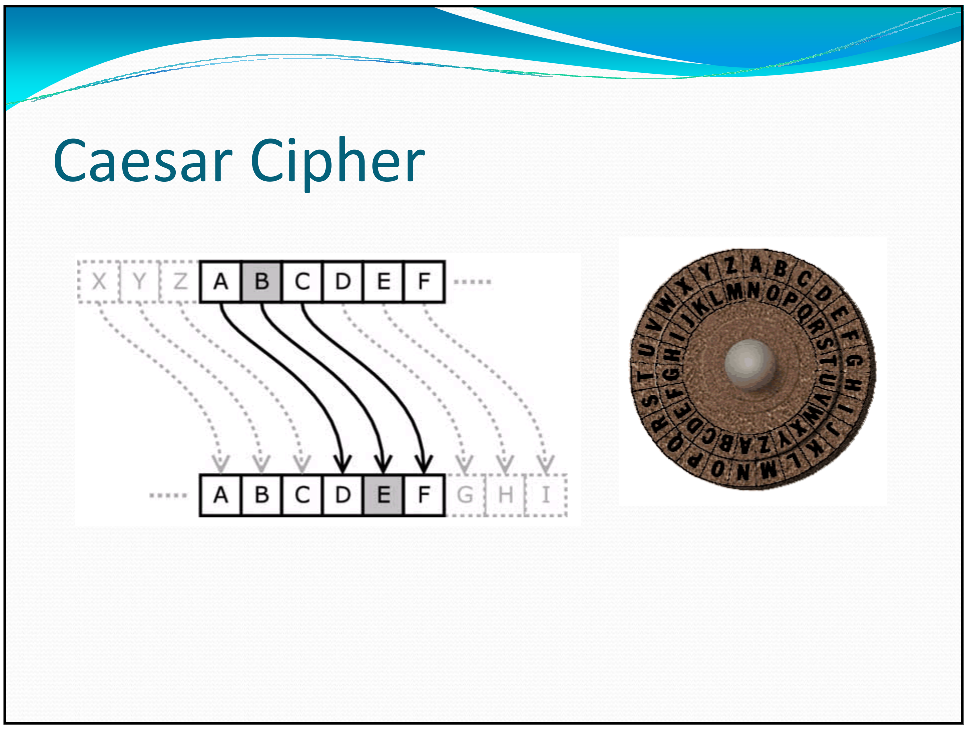
- **Encryption**: The rendering of information into a different which allow only the related parties to understand the contents.
- **Decryption**: The process to translate the blocked of received information from encryption to the receiver.

- Why we need this ? Discussion.

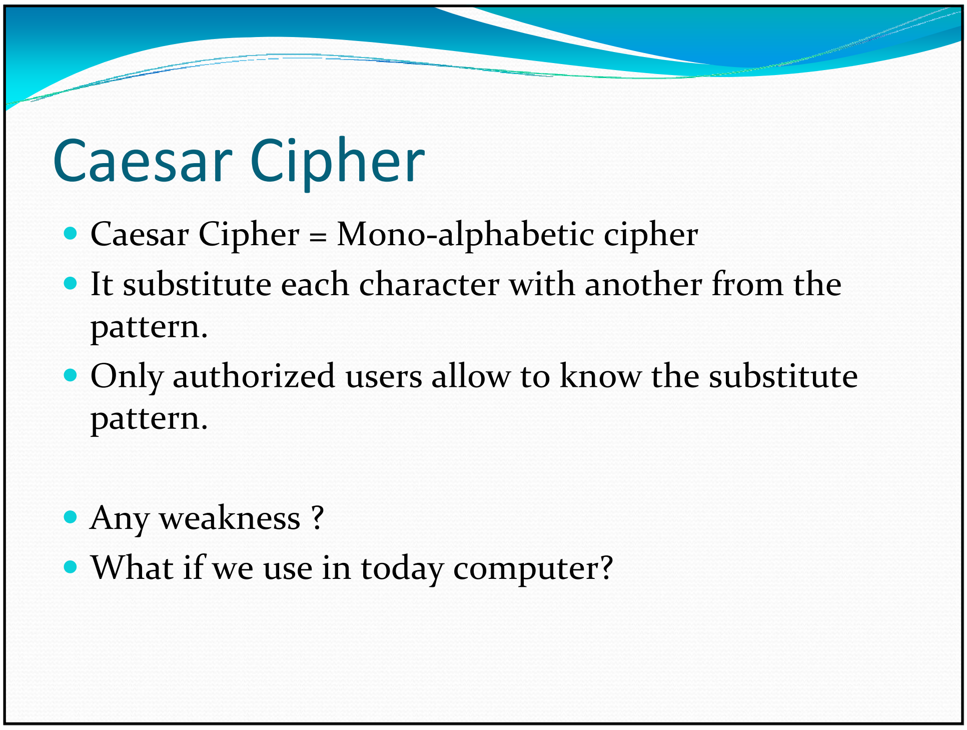


Data Security and Encryption

- Encryption and Decryption
  - **Caesar Cipher**
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking



Caesar Cipher



Caesar Cipher

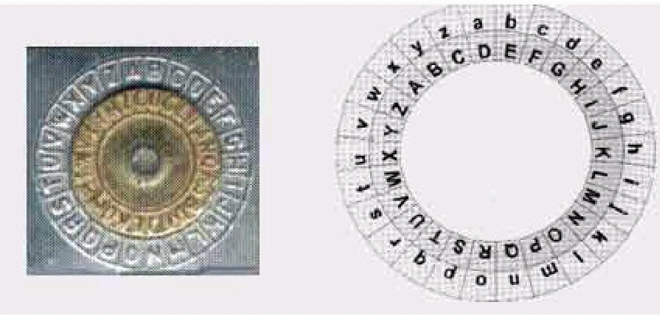
- Caesar Cipher = Mono-alphabetic cipher
- It substitute each character with another from the pattern.
- Only authorized users allow to know the substitute pattern.

- Any weakness ?
- What if we use in today computer?

Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - **Poly-alphabetic Cipher**
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking

Poly-alphabetic Cipher



Poly-alphabetic Cipher

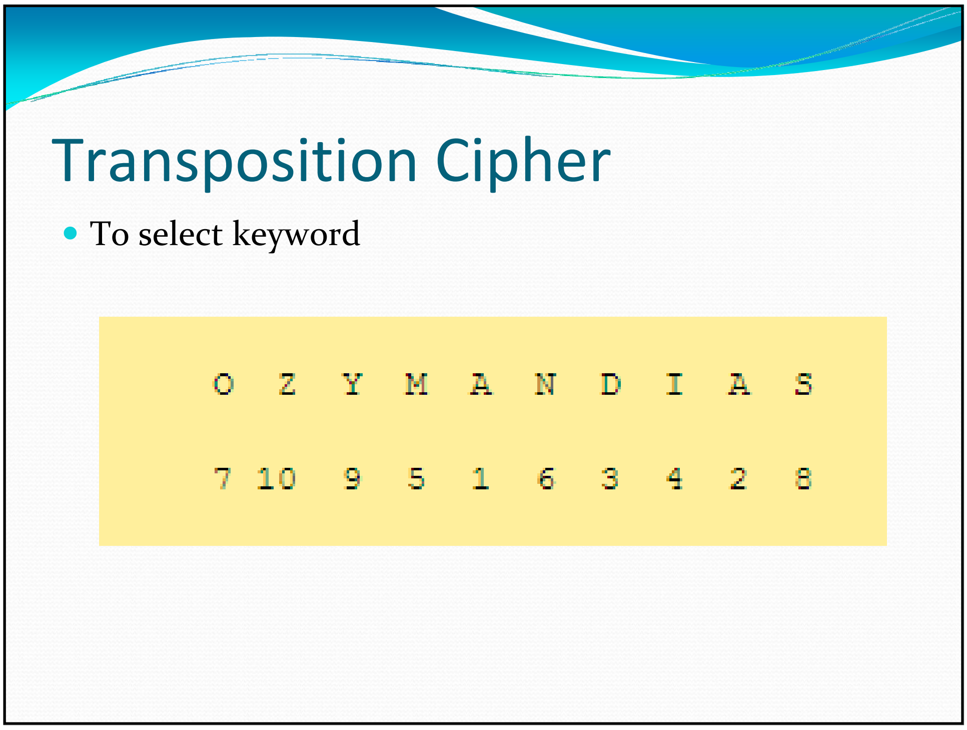
- Poly-alphabetic cipher: improved from mono-alphabetic cipher.
- It replaces each character with another.
- But, not always replaced with the same one.

- E.g Keyword CAB= 312
- Encoding word “AAA” -> “DBC”

- Does this cipher suit for today computer ? Why ?

Data Security and Encryption

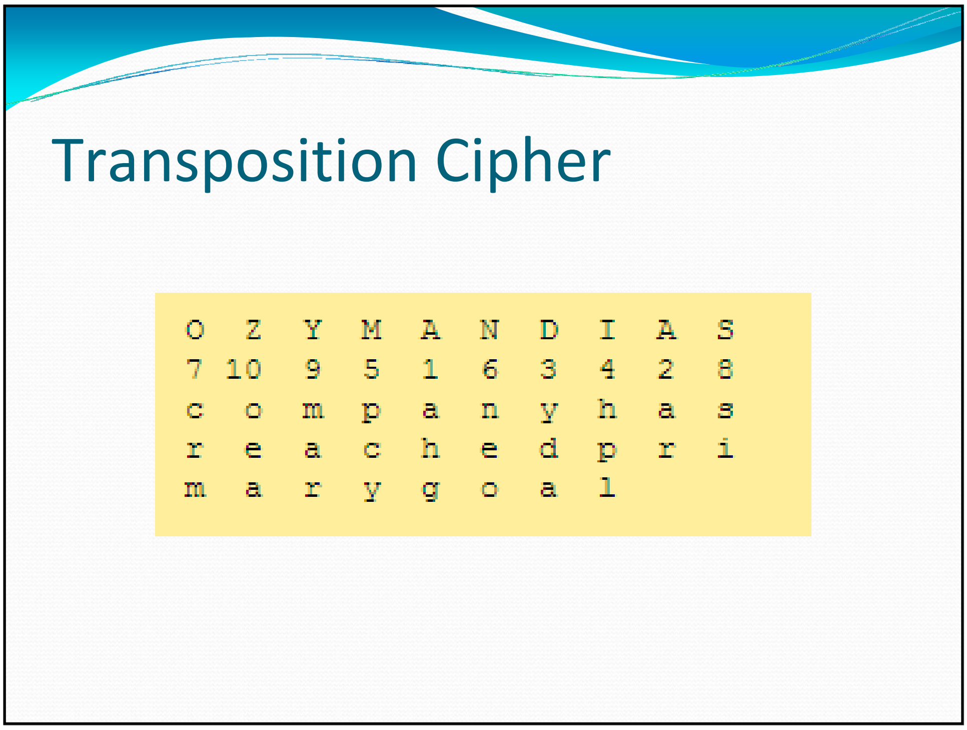
- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - **Transposition Cipher**
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking



Transposition Cipher

- To select keyword

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8



Transposition Cipher

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8
c	o	m	p	a	n	y	h	a	s
r	e	a	c	h	e	d	p	r	i
m	a	r	y	g	o	a	l		

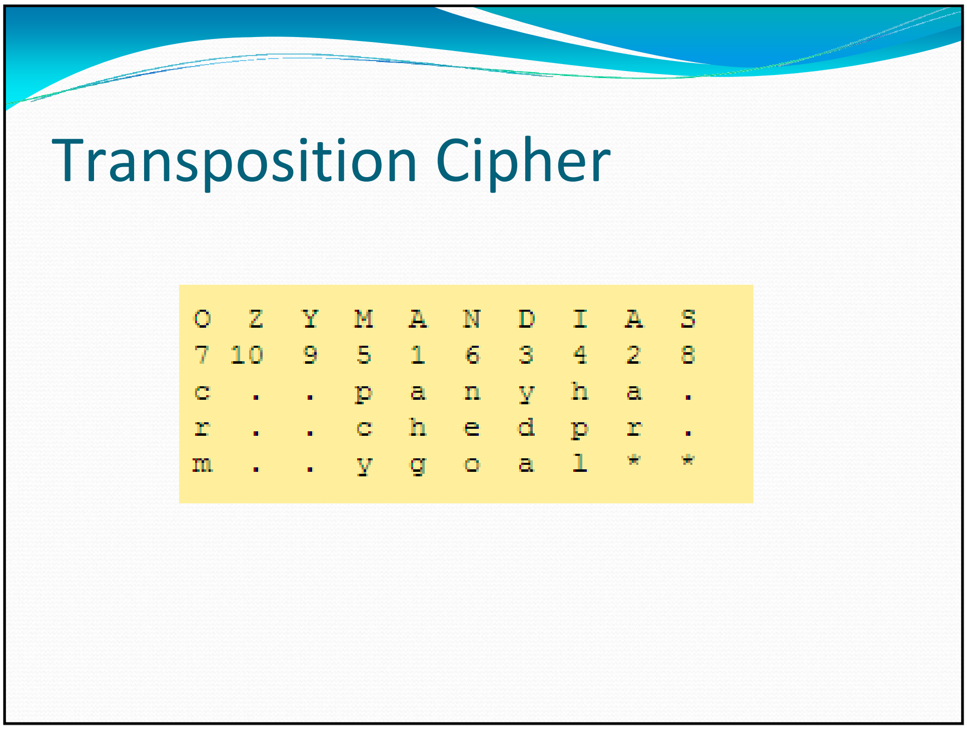
Transposition Cipher

AHGAR YDAHP LPCYN EOCRM SIMAR OEA

Transposition Cipher

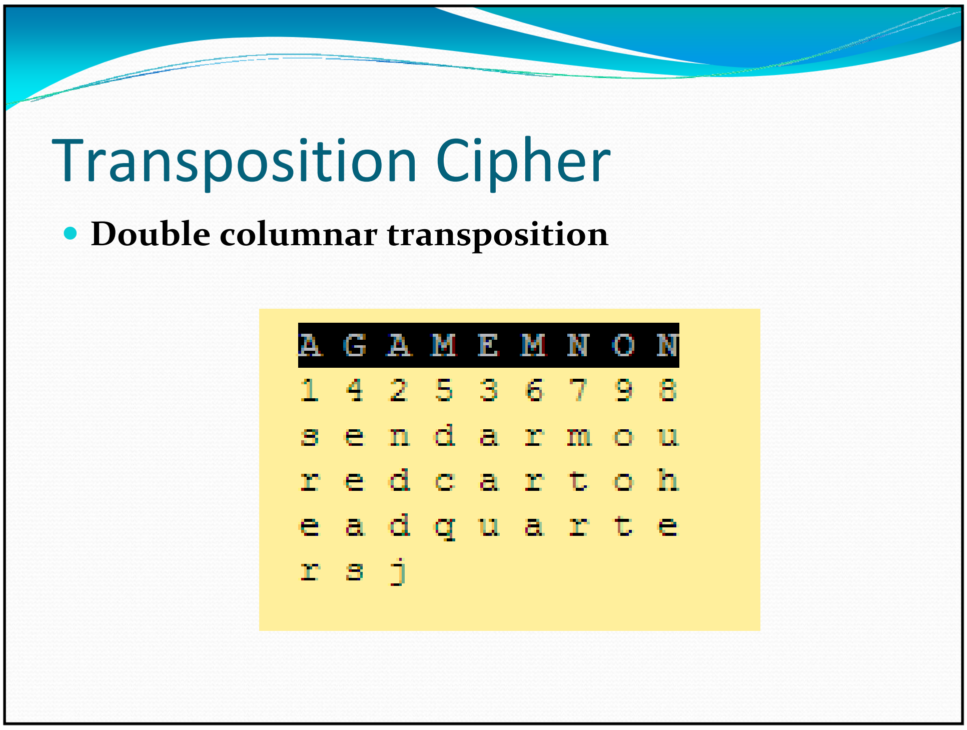
Decryption

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8
.	.	.	.	a	.	.	.	.	.
.	.	.	.	h	.	.	.	.	.
.	.	.	.	g	.	.	.	*	*



Transposition Cipher

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8
c	.	.	p	a	n	y	h	a	.
r	.	.	c	h	e	d	p	r	.
m	.	.	y	g	o	a	l	*	*



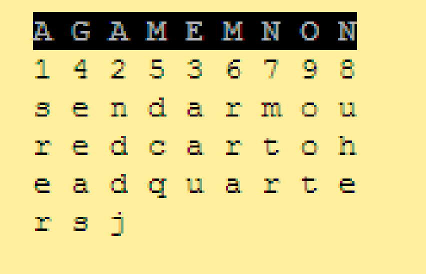
Transposition Cipher

- **Double columnar transposition**

A	G	A	M	E	M	N	O	N
1	4	2	5	3	6	7	9	8
s	e	n	d	a	r	m	o	u
r	e	d	c	a	r	t	o	h
e	a	d	q	u	a	r	t	e
r	s	j						

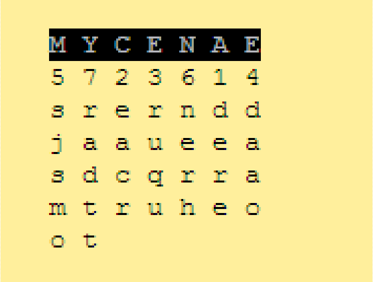
Transposition Cipher

- **Double columnar transposition**



A	G	A	M	E	M	N	O	N
1	4	2	5	3	6	7	9	8
s	e	n	d	a	r	m	o	u
r	e	d	c	a	r	t	o	h
e	a	d	q	u	a	r	t	e
r	s	j						

→

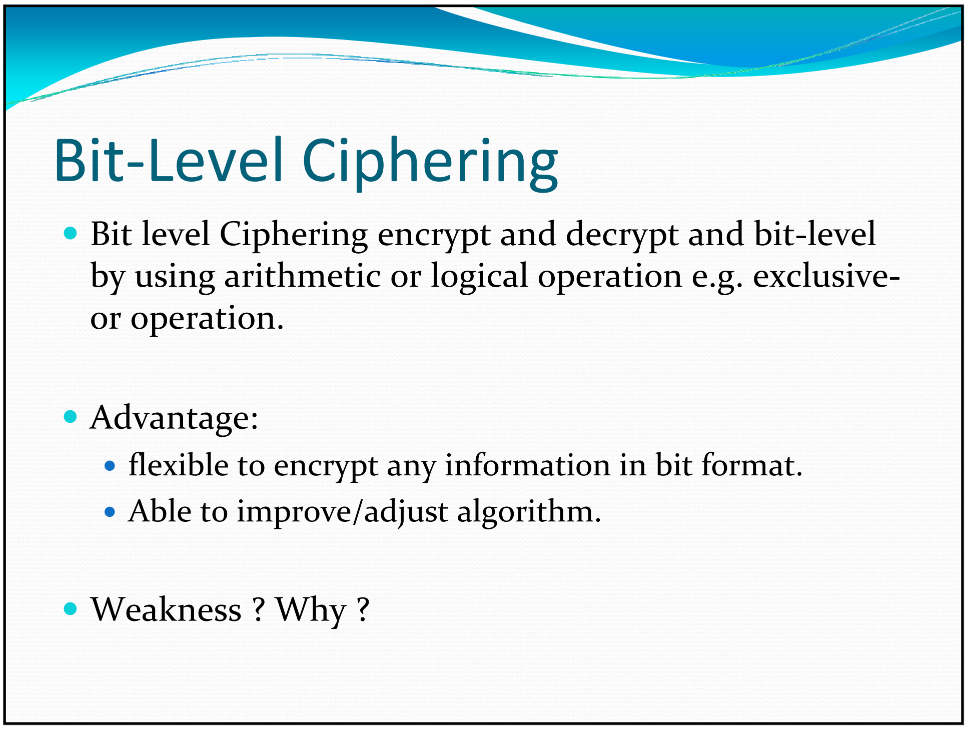


M	Y	C	E	N	A	E
5	7	2	3	6	1	4
s	r	e	r	n	d	d
j	a	a	u	e	e	a
s	d	c	q	r	r	a
m	t	r	u	h	e	o
o	t					

- DEREE ACRRU QUDAA OSJSM ONERH RADTT

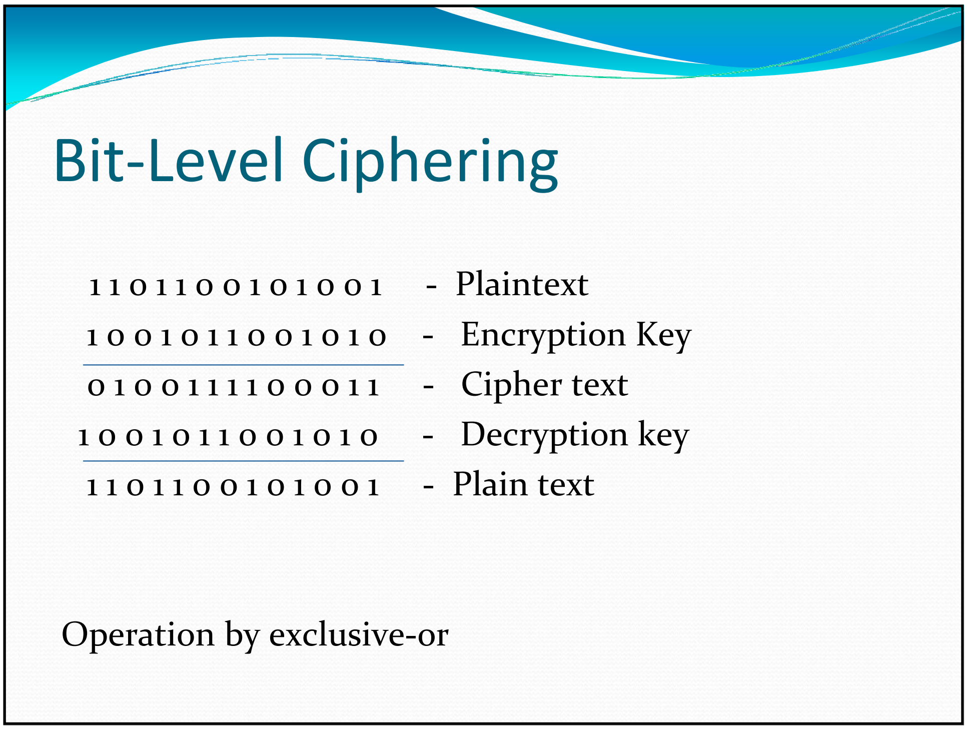
Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - **Bit-Level Ciphering**
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking



Bit-Level Ciphering

- Bit level Ciphering encrypt and decrypt and bit-level by using arithmetic or logical operation e.g. exclusive-or operation.
- Advantage:
  - flexible to encrypt any information in bit format.
  - Able to improve/adjust algorithm.
- Weakness ? Why ?



Bit-Level Ciphering

1 1 0 1 1 0 0 1 0 1 0 0 1	- Plaintext
1 0 0 1 0 1 1 0 0 1 0 1 0	- Encryption Key
0 1 0 0 1 1 1 1 0 0 0 1 1	- Cipher text
1 0 0 1 0 1 1 0 0 1 0 1 0	- Decryption key
1 1 0 1 1 0 0 1 0 1 0 0 1	- Plain text

Operation by exclusive-or

Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - **Data Encryption Standard**
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking

Data Encryption Standard

- To achieve sending and receiving data correctly.
- To reduce transferring algorithm between sender & receiver.
- But require to share with the public.
- Everyone can obtain encrypt & decrypt.
- So what do you think ?

Data Encryption Standard

Symmetric

- DES 64 bit, 128 bit ….
- AES …

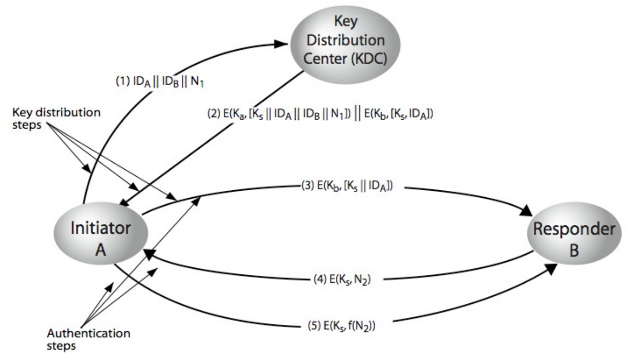
Asymmetric

- RSA
- Public key …

Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - **Key Distribution and Protection**
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking

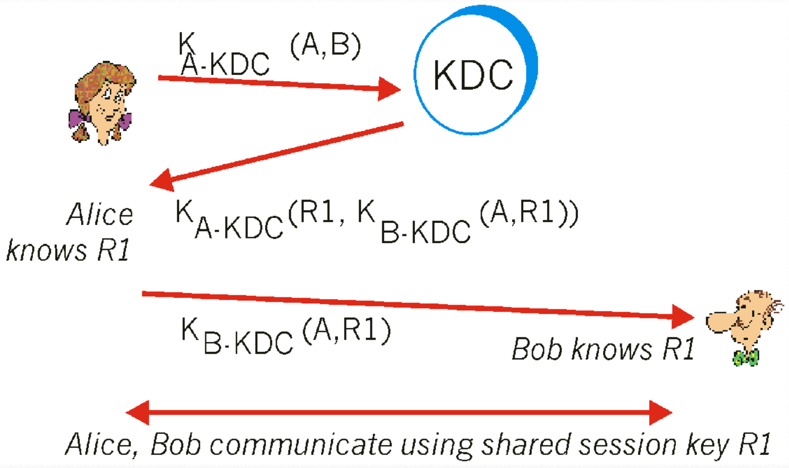
KDC Concept & Architecture


Key Distribution Center (KDC)
(1) $ID_A || ID_B || N_1$
(2) $E(K_a, [K_s || ID_A || ID_B || N_1]) || E(K_b, [K_s, ID_A])$
Key distribution steps
(3) $E(K_b, [K_s || ID_A])$
Initiator A
Responder B
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps

KDC Concept & Architecture

- hierarchies of KDC’s required for large networks, but must trust each other
- session key lifetimes should be limited for greater security
- use of automatic key distribution on behalf of users, but must trust system
- use of decentralized key distribution
- controlling key usage

KDC Concept & Architecture


$K_{A\text{-}KDC}(A,B)$
KDC
Alice knows R1
$K_{A\text{-}KDC}(R1, K_{B\text{-}KDC}(A,R1))$
$K_{B\text{-}KDC}(A,R1)$
Bob knows R1
Alice, Bob communicate using shared session key R1

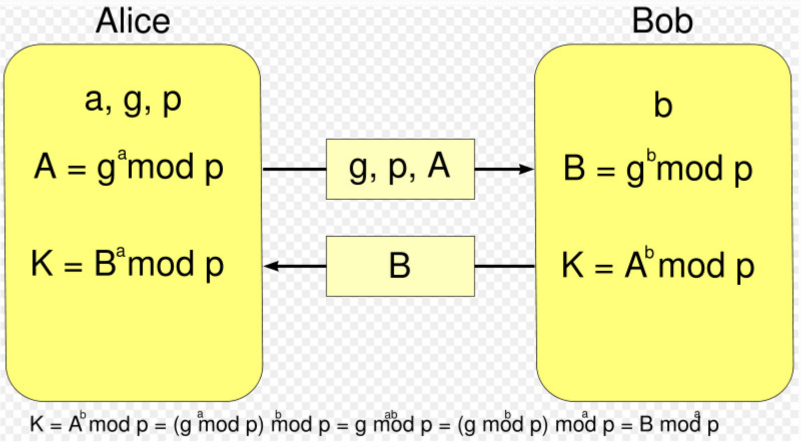
Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- **Public Key Encryption**
  - RSA Algorithm
  - Digital Signatures
- Viruses, Worms and Hacking

Diffie-Hellman

Diffie-Hellman key exchange (D-H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Diffie-Hellman



Alice

a, g, p

$A = g^a \bmod p$

$K = B^a \bmod p$

g, p, A

B

Bob

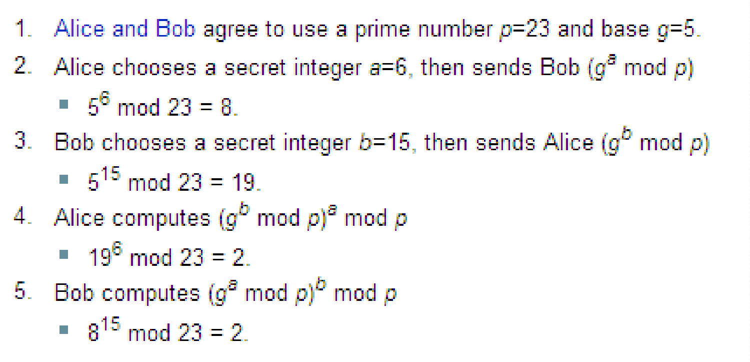
b

$B = g^b \bmod p$

$K = A^b \bmod p$

$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Diffie-Hellman



1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer a=6, then sends Bob (g^a mod p)
   - 5^6 mod 23 = 8.
3. Bob chooses a secret integer b=15, then sends Alice (g^b mod p)
   - 5^{15} mod 23 = 19.
4. Alice computes (g^b mod p)^a mod p
   - 19^6 mod 23 = 2.
5. Bob computes (g^a mod p)^b mod p
   - 8^{15} mod 23 = 2.

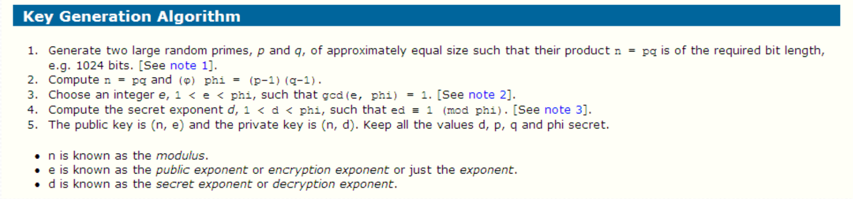
Diffie-Hellman

- Strength ?
  - Strong protocol
  - Do not have to reveal the secret code
- Weakness ?
  - Man in the middle attack.
  - Authentication
  - Complexity

Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - **RSA Algorithm**
  - Digital Signatures
- Viruses, Worms and Hacking

Rivest, Shamir, Adelman (RSA)

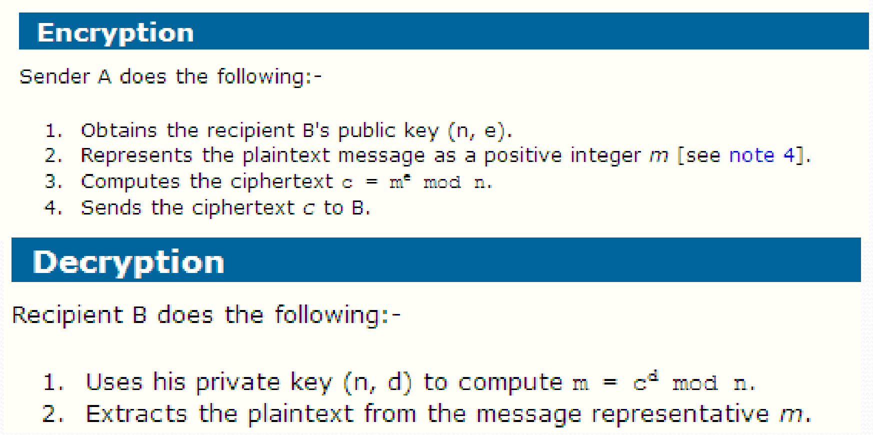


Key Generation Algorithm

1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product `n = pq` is of the required bit length, e.g. 1024 bits. [See note 1].
2. Compute `n = pq` and `(φ) phi = (p-1)(q-1)`.
3. Choose an integer *e*, `1 < e < phi`, such that `gcd(e, phi) = 1`. [See note 2].
4. Compute the secret exponent *d*, `1 < d < phi`, such that `ed ≡ 1 (mod phi)`. [See note 3].
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

Rivest, Shamir, Adelman (RSA)



Encryption

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer *m* [see note 4].
3. Computes the ciphertext $c = m^e \bmod n$.
4. Sends the ciphertext *c* to B.

Decryption

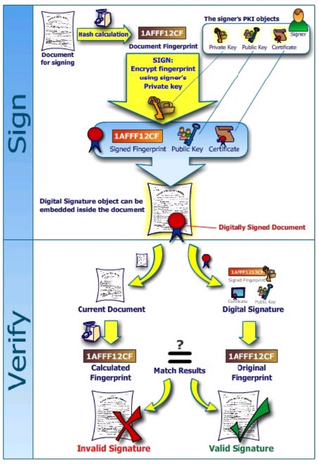
Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the message representative *m*.

Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - **Digital Signatures**
- Viruses, Worms and Hacking

What is Digital Signature?

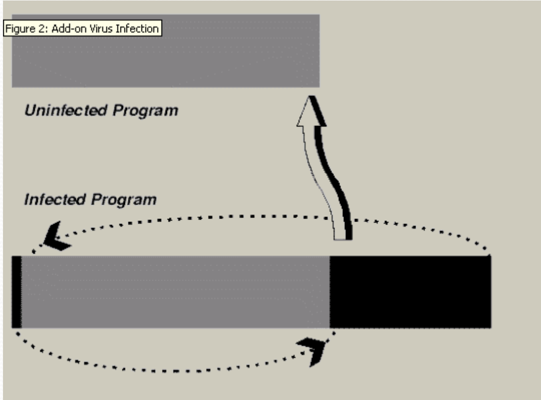


Data Security and Encryption

- Encryption and Decryption
  - Caesar Cipher
  - Poly-alphabetic Cipher
  - Transposition Cipher
  - Bit-Level Ciphering
  - Data Encryption Standard
  - Key Distribution and Protection
- Public Key Encryption
  - RSA Algorithm
  - Digital Signatures
- **Viruses, Worms and Hacking**

Viruses, Worms and Hacking

- Infecting



Q & A