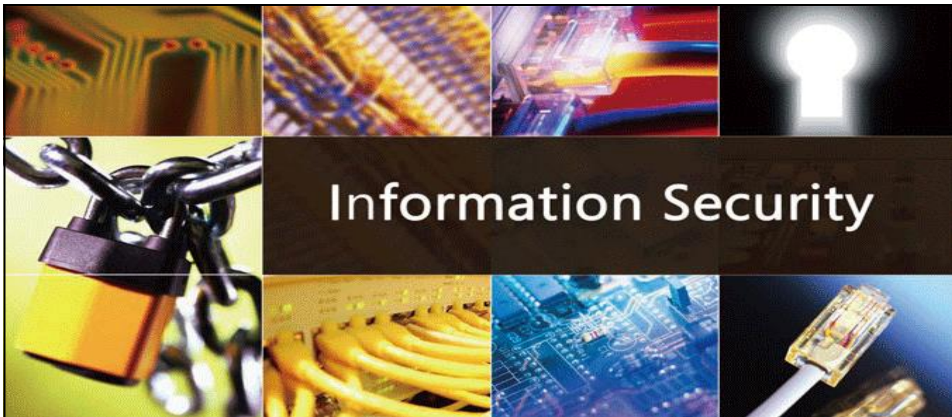


Introduction to Cryptography

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- **History of Encryption**
- **Substitution Techniques:** Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Polyalphabetic Ciphers
- **Transposition Techniques: Rail Fence**
- **Symmetric and asymmetric encryption**
- **Hash**
- **Digital signatures**

History of Encryption

- **Classical cryptography**
  - History of cryptography is over than 3,000 years
  - The object of the cryptography is **characters**
  - Encryption/Decryption is performed manually or by using mechanical principles
  - Applied commonly in military
    - A series of three rotors from an Enigma machine, used by Germany Military during World War II

3

History of Encryption

- **Modern cryptography (since 1970)**
  - Beginning with the development of Computer and Information Technology
  - Processing by Computer using **bits**
  - Applying widely in many fields, especially in electronic transactions

4

Cryptography in Action

- Some examples of applied cryptography are:
  - Public key infrastructure (PKI)
  - Digital certificates
  - Authentication
  - E-commerce
  - RSA
  - MD-5
  - Secure Hash Algorithm (SHA)
  - Secure Sockets Layer (SSL)
  - Pretty Good Privacy (PGP)
  - Secure Shell (SSH)

Main terms used in cryptography

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

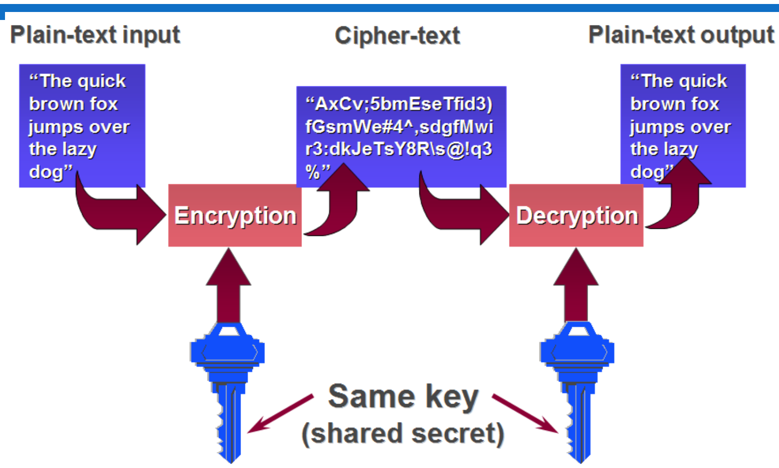
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm.

- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.

- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

So How Does It Work?



- There is a **one-to-one mapping**
- Provides **confidentiality protection**

Applications of Cryptography

- Goal: confidentiality
- Internet Protocol Security (IPSec):
  - a set of protocols designed (to operate at the Network layer of the OSI) to protect the confidentiality and integrity of data as it flows over a network.
- Pretty Good Privacy (PGP):
  - Using public key encryption, PGP is one of the most widely recognized cryptosystems in the world.
  - PGP has been used to protect the privacy of e-mail, data
- Secure Sockets Layer (SSL).
  - was developed by Netscape in the mid-1990s and rapidly became a standard mechanism for exchanging data securely over insecure channels such as the Internet.

Symmetric encryption model

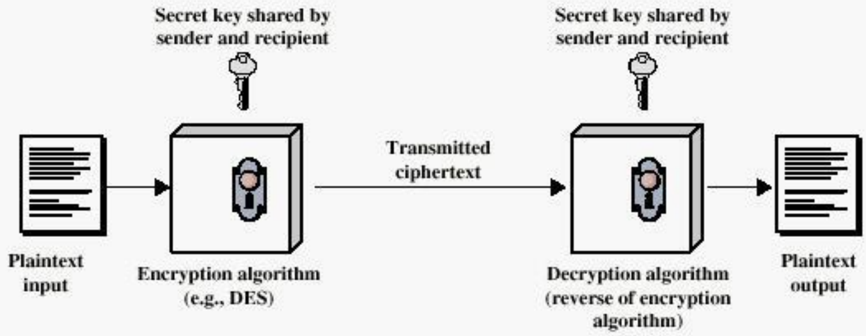
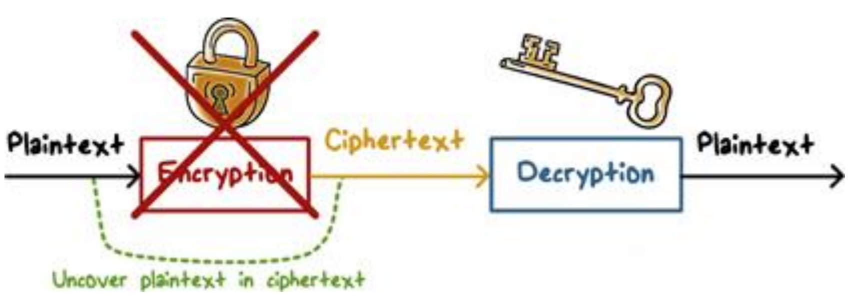


Figure 2.1 Simplified Model of Conventional Encryption

05/09/2017 9

Attacks on Encryption

- **Break a cipher:**
  - **Uncovering** plaintext *p* from ciphertext *c*, or, alternatively, **discovering** the key



Attacks on Encryption

- **Brute-force attack**
  - E.g., try all possible keys
- **Cryptanalysis**
  - Analysis of the algorithm and data characteristics
- **Implementation attacks**
  - E.g., side channel analysis
- **Social-engineering attacks**

Cryptanalysis and Brute-Force Attack

There are two general approaches to attacking a conventional encryption scheme

Brute-force attack

- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success

Cryptanalysis

- Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

types of cryptanalytic attacks

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cipher Strength

- A strong algorithm that meets 1 or 2 of the following criteria:
  - The cost of breaking the cipher exceeds the value of the encrypted information. (Low value)
  - The time required to break the cipher exceeds the useful lifetime of the information. (large time)
- Average Time Required for Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Taxonomy of Cryptography

The type of operations used for transforming plaintext to ciphertext
- Substitution
- Transposition

The number of keys used
- Symmetric, single-key, secret-key, conventional encryption
- Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed
- Block cipher
- Stream cipher

Substitution & Transposition

The type of operations used for transforming plaintext to ciphertext

- Substitution: Plaintext (bit pattern) are replaced by other letters or by numbers or symbols
  - Caesar
  - Monoalphabetic
  - Playfair
  - Polyalphabetic Vigenère
- Transposition: Perform some sort of permutation on the plaintext letters.
  - Rail fence

05/09/2017 16

Substitution Technique

Nguyen Thi Thanh Van - Khoa CNTT

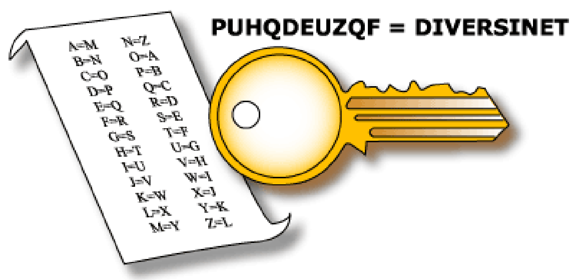
05/09/2017

Substitution Technique

- Caesar Cipher,
- Monoalphabetic Ciphers,
- Playfair Cipher,
- Polyalphabetic Ciphers

Caesar Cipher: introduction

- Caesar Cipher: invented by Julius Caesar
  - The earliest known,
  - The simplest,
  - use of a substitution cipher



Caesar Cipher: algorithm

- For each plaintext letter ***p***, substitute the ciphertext letter **C**, a shift parameter ***k*** is used as the key

- The encryption algorithm

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

  where k takes on a value in the range 1 to 25.

- The decryption algorithm is simply

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

- Ex: Decryption: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ . K=3

Caesar Cipher: Cryptanalysis

- The Caesar cipher can be easily broken by Brute-Force Method:
  - simply try all the 25 possible keys
- 3 important characteristics of cryptanalysis:
  - The encryption and decryption algorithms are known.
  - There are only 25 keys to try.
  - The language of the plaintext is known and easily recognizable (abbreviated or compressed)

Cryptanalysis

- Brute-Force Cryptanalysis of Caesar Cipher
- Ex: Decryption

PHHW PH DIWHU WKH WRJD SDUWB

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Monoalphabetic Ciphers

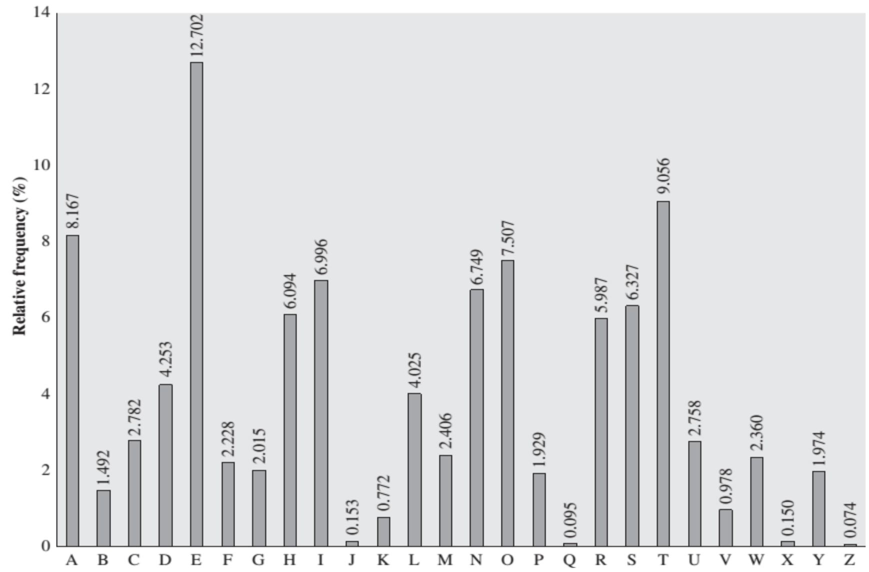
- The Caesar cipher is far from secure: only 25 possible keys
- A dramatic increase in the key space can be achieved by allowing an **arbitrary substitution**
- That is a monoalphabetic substitution cipher:
  - a single cipher alphabet is used per message
- Permutation
  - Of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once
- If the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys

Monoalphabetic Ciphers: Cryptanalysis

- Easy to break by Brute Force because they reflect the *frequency data* of the original alphabet:
  - Single letter: One-letter: ***e***
  - Digram: two-letter combination. Most common is ***th, an, ed***
  - Trigram: Three-letter combination. Most frequent is ***the, ing, est***
- *Ex: plaintext:*

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPO
PDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Monoalphabetic Ciphers



Monoalphabetic Ciphers: Cryptanalysis

- the *<u>frequency data: (single):</u>* E,t,a,o,I,s,h,r….
- *Ex: plaintext:* P:13, Z:11, Z:8….

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a         e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the    t
```

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

26

Playfair Cipher

- Invented by British scientist Sir Charles Wheatstone in **1854** (name of his friend - Baron Playfair)
- Best-known *multiple*-letter encryption cipher
- Treats diagrams in the plaintext as single units and translates these units into ciphertext digrams
  - Ex: lo ve => dg tu
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

Playfair Cipher: process

- Ex, using the keyword MONARCHY

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

- Process:
  - Fill in letters of keyword *from left to right* and *from top to bottom*, step another letter if a *letter repeated*
  - Fill in the remainder of the matrix with the remaining letters in alphabetic order
  - Note: I & J: same cell

Playfair Cipher: Encrypting

- Plaintext is encrypted *two letters* at a time, the following rules:
  - If a pair is a *repeated letter*, insert filler like 'X'
    ex: balloon -> ba lx lo on
  - If both letters fall in the *same row*, replace each with letter to **right** (wrapping back to start from end)
  - If both letters fall in the *same column*, replace each with the letter **below** it (wrapping to top from bottom)
  - *Otherwise* each letter is replaced by the letter in the same row and in the column of the other letter of the pair
  - ex

Playfair Cipher: ex

- Message = Move forward
- Plaintext = mo ve fo rw ar dx
- message is *padded* and *segmented*

x is just a filler

Cipher	Positions	Ciphertext
mo	same rows	mo → ON
ve	diffent rows and columns	ve → UF
fo	same column	fo → PH
rw	diffent rows and columns	rw → NZ
ar	same row	ar → RM
dx	diffent rows and columns	dx → BZ

- Ciphertext = ON UF PH NZ RM BZ

PlayFair cipher: Decrypting

- According to the letters positions in the grid :
  - if the 2 letters are on the same line, replace them by the ones on their **left** (loop to the right if the edge of the grid is reached),

  Ex, DE is decrypted CD.
  - if the 2 letters are on the same column, replace them by the ones just **above** (loop to the bottom if the top of the grid is reached),

  Ex, FK is decrypted AF.
  - If the 2 letters are similar (same column, same line), replace it by ones on their **left and above**.
  - else, replace the letters by the ones forming a rectangle with the original pair. Beginning with the letter on the same line as the first letter to crypt. L^1L^2 => $L1=(rowL^1,colL^2)$; $L2= =(rowL^2,colL^1)$;

  Ex, BF is decrypted AG; GA is decrypted FB

PlayFair cipher, ex

*	*	*	*	*
*	A	B	C	D
*	E	G	H	P
*	*	R	S	*
*	T	U	X	Z

- Ex1: EC -> HA, BC -> AB, RU -> GR, **XX->RR**

Playfair Cipher: Security

- Security *much improved* over monoalphabetic
- Since have 26 x 26 = 676 digrams
- Would need a 676 entry frequency table to analyze (versus 26 for a monoalphabetic)
- Correspondingly more ciphertext was widely used for for many years eg. by US & British military in WW1
- It can be broken, given a few hundred letters
- Since still has much of plaintext structure

Vigenère Cipher

- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a *key letter* which is the ciphertext letter that substitutes for the plaintext letter

Vigenère Cipher Table

Key

plain text

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

Vigenère Cipher: Example

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a *repeating keyword*
  For example, if the keyword is *deceptive*,
- the message "we are discovered save yourself" is encrypted:
- key: d e c e p t i v e d e c e p t i v e d e c e p t i v e
- plaintext: w e a r e d i s c o v e r e d s a v e y o u r s e l f
- ciphertext: Z I C V T WQNGRZGVTWAVZHCQYGLMGJ
- It works as follows: (look into Vigenère table)
  - Row d + column w -> Z
  - Row e + column e -> I

Vigenère Cipher: Decrypto

- One locates the first letter of the key in the left column, and locates on the row the first letter of the ciphered message. Then go up in the column to read the first letter, it is the corresponding plain letter.
- One continues with the next letters of the message and the next letters of the key, when arrived at the end of the key, go back the the first key of the key.

Vigenère Cipher: ex

- Ex: K= KEY. C= NGMNI.
  - Locates the letter K on the first column, and on the row of it, find the cell of the letter N, the name of its column is D, it is the first letter of the plain message.
  - continues
  - The original plain text is DCODE.

Transposition technique

Nguyen Thi Thanh Van - Khoa CNTT

05/09/2017

Rail fence

- **Rail fence** technique: the simplest such cipher
  - the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
  - For example, to encipher the message "meet me after the toga party" with a rail fence of **depth 2**, we write the following:

    m e m a t r h t g p r y
     e t e f e t e o a a t

  - The encrypted message is: MEMATRHTGPRYETEFETEOAAT
  - Dencrypted ?

Transposition technique

- A more complex scheme:
  - write the message in a rectangle,
  - row by row, and read the message off,
  - column by column, but permute the order of the columns.
  - The **order of the columns** then becomes the **key** to the algorithm.
- For example,

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

- Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

05/09/2017 41

Taxonomy of Cryptography

The type of operations used for transforming plaintext to ciphertext

- Substitution
- Transposition

The number of keys used

- Symmetric, single-key, secret-key, conventional encryption
- Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed

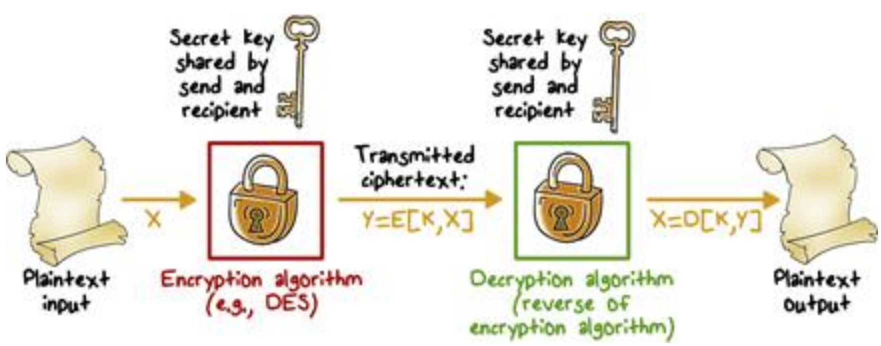
- Block cipher
- Stream cipher

Symmetric & Asymmetric Encryption

- **Secret key cryptography: one key** same key for encryption and decryption
- **Public key cryptography (**Asymmetric) **: two keys**
  - **Public - key**,
    - everyone can know and
    - use to **encrypt the message** or
    - to **check the signature** of key's owner.
  - **Private – key**:
    - only owner knows and
    - use to **decrypt the message** or
    - to **create the signature**
- Public for encryption, private for decryption
- Private for signing and public for verification

06/09/2017 43

Symmetric Encryption



Comparison of Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

A block cipher:
- processes the plaintext input in fixed-size blocks
- produces a block of ciphertext of equal size for each plaintext block.

Comparison of Encryption Algorithms

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 descryptions/s	Time Required at 10 descryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.3×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 5.3×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 5.3×10^{60} years	1.8×10^{56} years

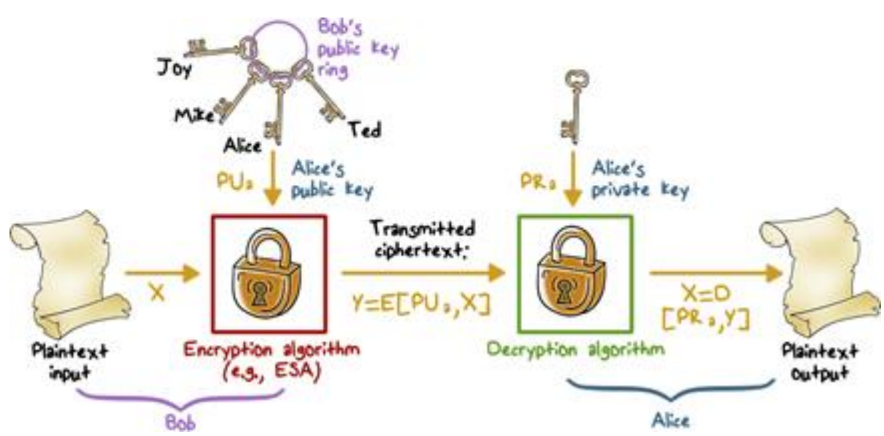
Symmetric Encryption Quiz

Select the correct definition for **each type of attack**:

A. A method to determine the encryption function by analyzing known phrases and their encryption
B. Analyzing the effect of changes in input on the encrypted output
C. Compare the ciphertexts with its known plaintext
D. A method where a specific known plaintext is compared to its ciphertext

- ☐ known-Plaintext attacks
- ☐ chosen-Plaintext attacks
- ☐ differential cryptanalysis
- ☐ linear cryptanalysis

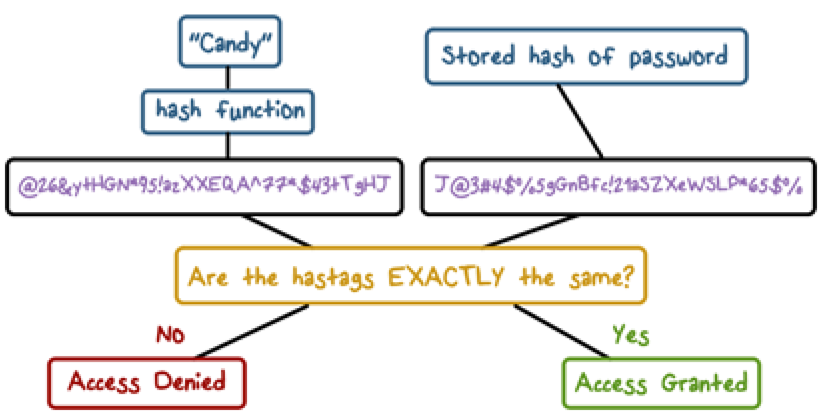
Asymmetric Encryption



Hash Functions

- Compute message digest of **data of any size**
- **Fixed length output**: 128-512 bits
- Easy to compute $H(m)$
- Given $H(m)$, no easy way to find m
  - ***One-way function***
- Given m_1, it is computationally infeasible to find $m_2 \neq m_1$ s.t. $H(m_2) = H(m_1)$
  - **Weak collision resistant**
- Computationally infeasible to find $m_1 \neq m_2$ s.t. $H(m_1) = H(m_2)$
  - **Strong collision resistant**

Hash Functions for Passwords

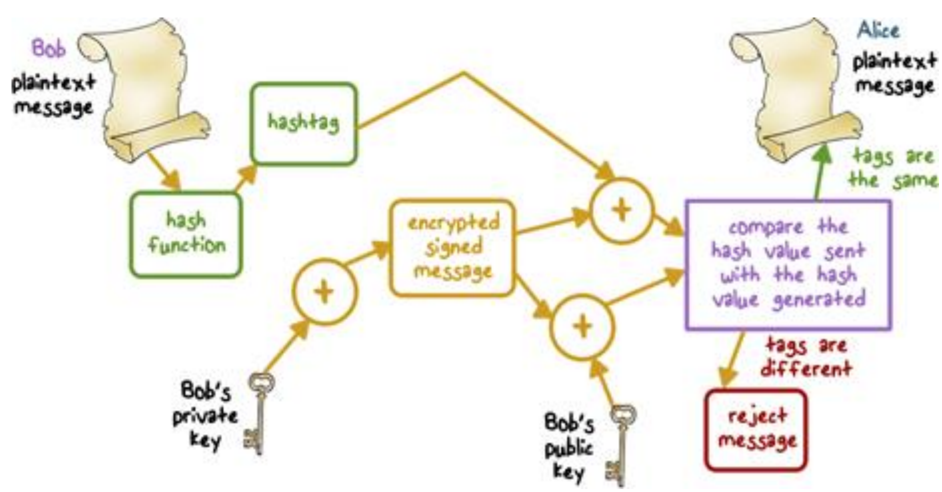


Hash Function Quiz

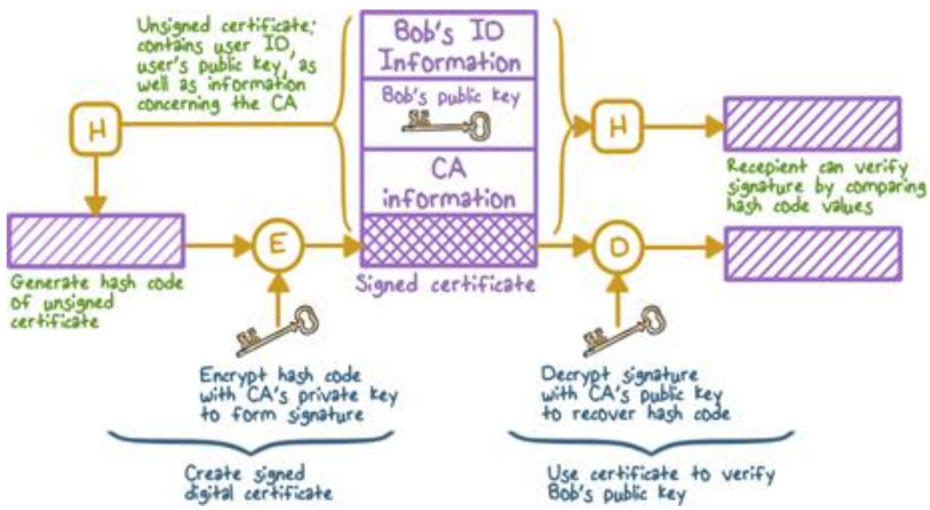
Which of the following characteristics would i**improve password security**?

- ☐ Use a one-way hash function
- ☐ Should not use the flood effect
- ☐ Should only check to see that the hash function output is the same as stored output

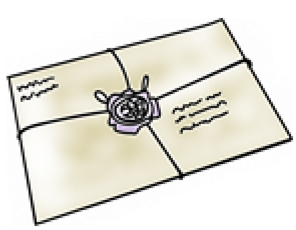
Digital Signatures



Digital Signatures

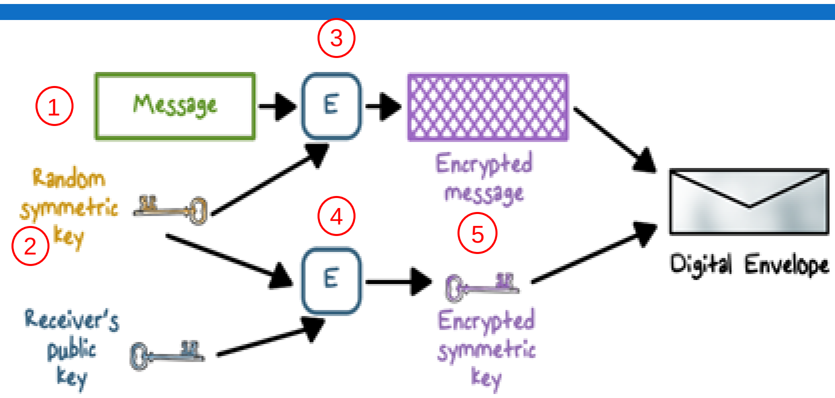


Digital Envelopes



- Means: public-key encryption is used to protect a symmetric key
- Protects a message **without needing** to first arrange for sender and receiver to have the same secret key
- Compares to the same thing as a **wrapped envelope containing an unsigned letter**

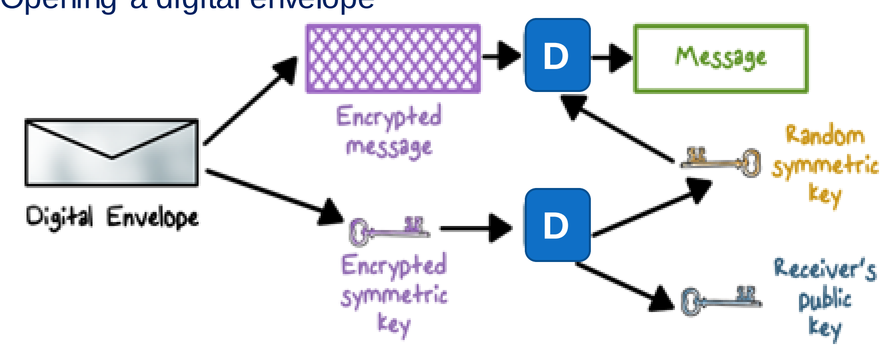
Digital Envelopes



1. Prepares a message.
2. Generates a random symmetric key that will be used this one time only.
3. Encrypts that message using symmetric encryption the one-time key.
4. Encrypts the one-time key using public-key encryption with Alice's public key.
5. Attaches the encrypted one-time key to the encrypted message and sends it

Digital Envelopes

Opening a digital envelope



Receiver is capable of decrypting the one-time key and recovering the original message. If Bob obtains Alice's public key by means of Alice's public-key certificate, then Bob is assured that it is a valid key.

Summary

- **History of Encryption**
- **Substitution Techniques:** Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Polyalphabetic Ciphers
- **Transposition Techniques: Rail Fence**
- **Symmetric and asymmetric encryption**
- **Hash**
- **Digital signatures**

References

- *2007, Cryptography and Network Security*, Principles and Practice, William Stallings, Prentice Hall, Fifth Edition,
  - Chapter 2,3,5,6,8,9,11,12,13
- 2014, *Cryptography and Network Security*, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition,
- 2014, CEHv8: Certified Ethical Hacker Version 8 Study Guide.
  - Chapter 2,3

Q & A