Security (CS4028)

Lecture 2. Introduction to Cryptography

Chunyan Mu

chunyan.mu@abdn.ac.uk

The School of Natural and Computing Sciences

Schedule

	Week	Lecture 1	Lecture 2	Tutorial
⇒	1	Intro to course & security	Intro to Crypto	-
	2	Symmetric Crypto	Hash	Math for crypto
	3	Asymmetric Crypto-1	Asymmetric Crypto-2	Symmetric Crypto
	4	Signatures	Zero Knowledge Proof	Asymmetric Crypto
	5	Certificates	Authentication	Signature & certificates
	6	Access Control	AC models	Authentication
	7	Information flow control	Information flow control	Access control
	8	Management	Protocols	Concepts & management
	9	Network security	Network security	Protocols and communications
	10	Advanced Topic	Advanced Topic	Network
	11	Revision		

Outline

Outline

Outline

Cryptography: definitions

The Greek origin of the word

- crypto - hidden/secret + grafia - writing
- "the science and study of secret writing"

Definitions

Cryptography is the science of protecting data, which provides means of converting data into unreadable form, so that

- the data cannot be accessed for unauthorised use
- the content of the data frames is hidden
- the authenticity of the data can be established
- the undetected modification of the data is avoided
- the data cannot be disowned by the originator of the message

Why Cryptography?

In general

Passing (secret) information through potentially insecure channels, such as:

- military campaign
- financial/online banking/shopping
- diplomatic communications (espionage)

Why Cryptography?

The four goals

In spite of adversaries, we want to achieve (among other things):

1. Confidentiality - prevent unauthorised access;
2. Integrity - no modification of existing information;
3. Authentication - no identifying either entities or data origins;
4. Non-repudiation - preventing denials of messages sent

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice

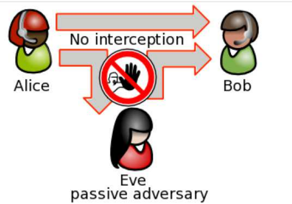
Confidentiality: no possible interception

Confidentiality

This comprises two separate requirements:

1. no observer can access the contents of the message;
2. no observer can identify the sender and receiver

The terms privacy or secrecy are also used to mean confidentiality

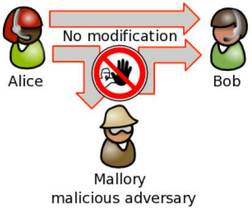


Integrity: no possible alteration

Integrity

This requires that the recipient can be sure that:

1. the message has not been changed or lost during transmission;
2. the message has not been prevented from reaching the recipient;
3. the message has not reached the recipient twice.

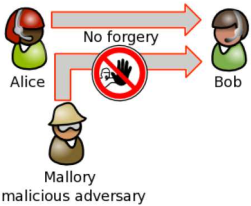


Authentication: no possible forgery

Authentication

This requires that:

1. the sender can be sure that the message reaches the intended recipient, and only the intended recipient; and
2. the recipient can be sure that the message came from the sender and not an imposter. The act by an imposter of sending such a message is referred to as "spoofing"



Availability: no possible deny

Non-repudiation

This requires that:

1. the sender cannot deny that the message was sent by him;
2. the recipient cannot deny that the message was received by him;

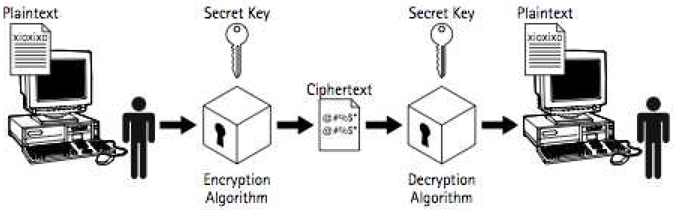
Terminology

Encryption

- Plain text (or clear text) - text that can be read by a human
- Encryption - process of transforming plaintext into ciphertext
- Cipher text (or encrypted text) - text that needs to be processed to be read by a human being
- Decryption - process of transforming a cipher text into a plain text (the reverse of encryption)
- Cipher - a secret method of writing (i.e., encryption scheme: mathematical function(s) or algorithm(s) used for encryption and decryption, they are usually using keys)
- Key - is a word, number, or phrase that is used to encrypt the clear text.

Conventional encryption model

1. A sender wants to send a "hello" message to a recipient.
2. The original message (plaintext) is converted to ciphertext by using a key and an algorithm.
3. The ciphertext is transmitted over the transmission medium.
4. At the recipient end, the ciphertext is converted back to the original text using the same algorithm and key that were used to encrypt the message.



Main cryptography techniques

Symmetric encryption

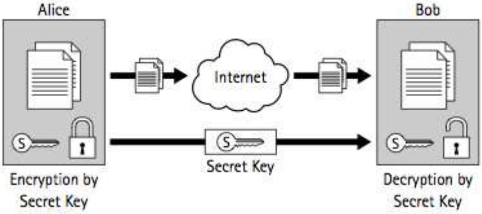
- known as secret key cryptography: $\mathcal{E}_k(PT) = CT$, $\mathcal{D}_k(CT) = PT$
- based on a single key: the same key is used to encrypt and decrypt the data

Non-symmetric encryption

- known as public key cryptography: $\mathcal{E}_{k_1}(PT) = CT$, $\mathcal{D}_{k_2}(CT) = PT$
- base on a combination of two keys - secret key and public key: public key is used for encryption, and the secret key is used for decryption

Main cryptography techniques

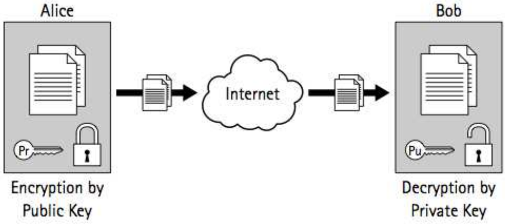
Symmetric (secret key) cryptography



- main problem: the sender and the receiver have to agree on a common key, a secure channel is also required exchange the secret key
- most widely used secret key algorithm: DES, 3DES, AES etc

Main cryptography techniques

Non-symmetric (public key) cryptography



- Non-symmetric: both keys are required to complete the process (encrypted by the public key and decrypted by the private key)
- widely used algorithm: RSA

Outline

Classical (Traditional) cryptographic techniques

Classification

- Two basic components of classical ciphers: substitution and transposition
  - substitution ciphers: letters are replaced by other letters
  - transposition ciphers: the letters are arranged in a different order
- These ciphers may be:
  - monoalphabetic - only one substitution/ transposition is used, or
  - polyalphabetic - where several substitutions/ transpositions are used
- several such ciphers may be concatenated together to form a product cipher

Substitution cipher

Caesar (50-60BC) - monoalphabetic

- ignore space character, gather letters in t-letter blocks
- rotate left or right by some number of positions to obtain cipher text.
- can describe this cipher as:
  - Encryption $\mathcal{E}_k : i \rightarrow i + k \mod 26$
  - Decryption $\mathcal{D}_k : i \rightarrow i - k \mod 26$

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
cipher text	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

Example

plain text	RETURN TO ROME	cipher text	VIXYV RXSVS QI
5-letter blocks	RETUR NTORO ME	-4 shift	RETUR NTORO ME
+4 shift	VIXYV RXSVS QI	interpretation	RETURN TO ROME

Substitution cipher

Monalphabetic substitution

- Caesar cipher generalisation, keyword used to permute the alphabet:
- Write keyword (no repeat characters), suppose keyword is `JACKSON`, followed by remainder of alphabet in order:

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

- What does your partner in crime need to encrypt/decrypt?
  - just the keyword
- How secure? i.e., how difficult to break?
  - letter frequency analysis is a good attack

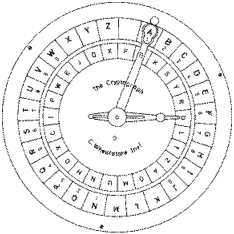
Example: monalphabetic substitution cipher

plain text	S E N D	R E I N F O R C E M E N T
cipher text	R S I K	Q S D I O L Q C S H S I T

Substitution cipher

Porta (1563) - monoalphabetic polygraphic

- Replace 2-letter blocks with corresponding symbols
- The first letter (key) is stationary while the second letter moves, indicating which symbol is to be used instead of the original 2-letter block



Substitution cipher

Porta: A matrix can easily represent the original disc ...

```
Keys| 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,B | 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
C,D | o p q r s t u v w x y z n m a b c d e f g h i j k l
E,F | p q r s t u v w x y z n o l m a b c d e f g h i j k
G,H | q r s t u v w x y z n o p k l m a b c d e f g h i j
I,J | r s t u v w x y z n o p q j k l m a b c d e f g h i
K,L | s t u v w x y z n o p q r i j k l m a b c d e f g h
M,N | t u v w x y z n o p q r s h i j k l m a b c d e f g
O,P | u v w x y z n o p q r s t g h i j k l m a b c d e f
Q,R | v w x y z n o p q r s t u f g h i j k l m a b c d e
S,T | w x y z n o p q r s t u v e f g h i j k l m a b c d
U,V | x y z n o p q r s t u v w d e f g h i j k l m a b c
W,X | y z n o p q r s t u v w x c d e f g h i j k l m a b
Y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a
```

- The 'key' for a porta cipher is a key word. e.g. 'FORTIFICATION'
- To encipher a message, repeat the keyword above the plaintext:

key	F	O	R	T	I	F	I	C	A	T	I	O	N	F	O	R	T	I	F	I	C	A	T	I	O	N	F	O
plain text	D	E	F	E	N	D	T	H	E	E	A	S	T	W	A	L	L	O	F	T	H	E	C	A	S	T	L	E
cipher text	s	y	n	n	j	s	c	v	r	n	r	l	a	h	u	t	u	k	u	c	v	r	y	r	l	a	n	y

Substitution cipher

Vigenere (1553) - polyalphabetic

The message is encrypted using the original plain text, a (text) key, and the table:

	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

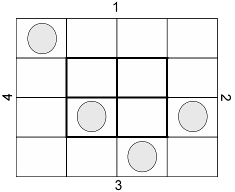
An example

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
key	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R
cipher text	C	S	A	S	X	T	I	Y	G	Y	D	Z	O	E	M	E	J	F	U	K	S	K	P	L	A	Q

Transposition cipher

Turning Grille (Fleissner, Wostrowitz 1881)

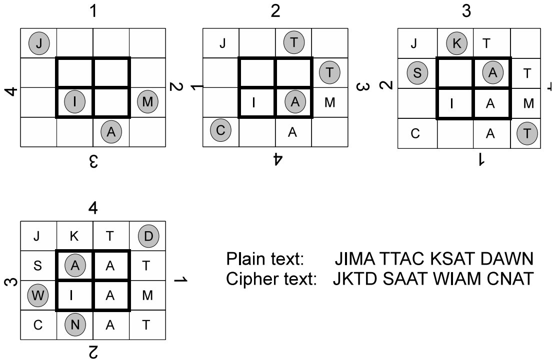
- This template was a square with a number of holes punched out.
- There are an even number of rows and columns (thus the total number of fields is divisible by 4).
- One fourth of these fields is cut out. This template is used for both encoding and decoding the message.



Transposition cipher

Example: Turning Grille

Encrypt `JIM ATTACKS AT DAWN` using this grille.



This system was used in World War II by German spies in South America.

Product cipher: a combination

Feistel-IBM-1971

- Predecessor for the Data Encryption Standard (DES).
- This system uses permutations (transpositions) on large blocks for the mixing transformation, and substitution on small blocks for confusion.
- This system is based on two hardware components:
  - P-box (Permutation box)
  - S-box (Substitution box)

Outline

Block Ciphers and Stream Ciphers

Block ciphers

- A type of symmetric-key encryption
- Transforms a fixed-length block of plaintext into a block of ciphertext of the same length, using a user provided secret key.
- Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key
- The fixed length is called the block size, and for many block ciphers, the block size is 64 bits.

Block Ciphers and Stream Ciphers

Stream ciphers

- A stream cipher generates a **keystream**, a sequence of bits used as a key
- Encryption: accomplished by combining the **keystream** with the plaintext, usually with the bitwise **XOR** operation
- The generation of the keystream can be independent of the plaintext and ciphertext, termed as **synchronous**
- Or it can depend on the data and its encryption, termed as **self-synchronising**
- Most stream cipher designs are for synchronous stream ciphers.

Stream Ciphers

Example: Vernam Cipher

- A Vernam cipher is a stream cipher in which the plaintext is XORed with a random or pseudorandom stream of data of the same length to generate the ciphertext
- If the stream of data is truly random and used only once, then the cipher is a one-time pad.

Encryption

	c	a	t
	01100011	01100001	01110100
$\oplus$	10110001	01010101	10111001
	11010010	00110100	11001101

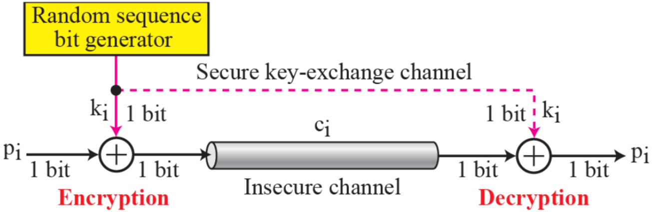
Decryption

	11010010	00110100	11001101
$\oplus$	10110001	01010101	10111001
	01100011	01100001	01110100
	c	a	t

Stream Ciphers

Example: One Time Pad

- The message is encrypted by combining (usually XORing) it with a perfectly random key at least as long as the message and the key is only used once.
- Apart from the problem of obtaining a perfectly random key, the main problem with one time pads is the distribution of keys.



Stream Ciphers vs. Block Ciphers

Stream cipher

- A type of symmetric encryption algorithm
- Can be designed to be exceptionally fast, much faster than any block cipher
- Typically operate on smaller units of plaintext, usually bits.
- The transformation of plaintext units will vary, depending on when they are encountered during the encryption process

Block cipher

- Operate on large blocks of data
- The encryption of any particular plaintext with will result in the same ciphertext when the same key is used

Outline

Cryptographic modes

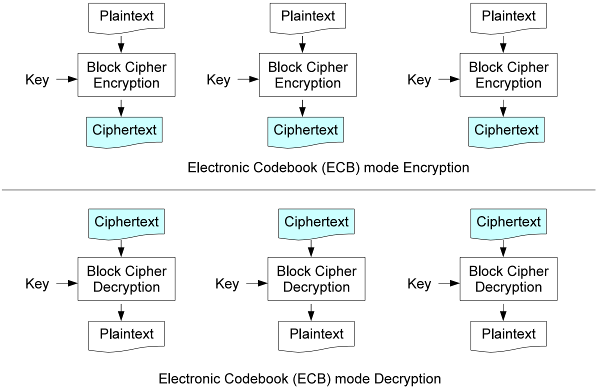
Four modes of operation

- A block cipher encrypts a plain text in fixed-size n-bit blocks (often $n = 64$)
- For messages exceeding n bit we can use four different modes of operation:
  - ECB: Electronic Code Block
  - CBC: Cipher-Block Chaining
  - CFB: Cipher FeedBack
  - OFB: Output FeedBack

Cryptographic modes

Electronic Code Block (ECB)

- the message is divided into blocks and each block is encrypted separately: $c_j = E_k(m_j)$



Cryptographic modes

Cipher-Block Chaining (CBC)

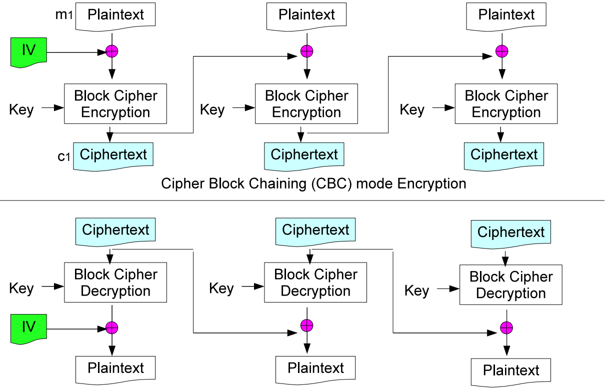
- a plain text block is XORed with the previous cipher text block before encryption
- the first plain text block is XORed with an Initializing Vector IV:

$$c_1 = E_k(m_1 \oplus IV)$$

- $c_j = E_k(m_j \oplus c_{j-1})$

Cryptographic modes

Cipher-Block Chaining (CBC)



Cipher Block Chaining (CBC) mode Encryption

Cipher Block Chaining (CBC) mode Decryption

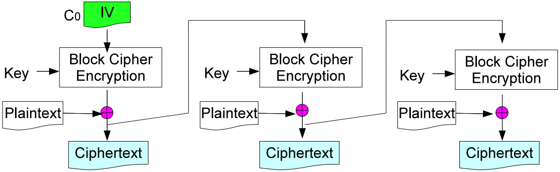
Cryptographic modes

Cipher FeedBack (CFB)

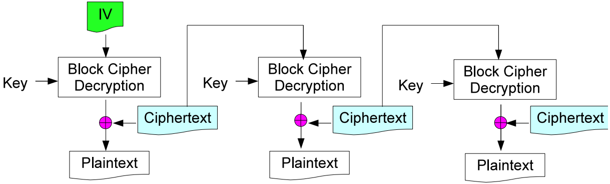
- plain text is encrypted in blocks of size r ($r < n$);
- the n-bit Shift Register (initially IV) is encrypted into an intermediate cipher text;
- the left-most r bits of the intermediate encrypted text are XORed with the next r bits of the plain text to obtain r bits of cipher text;
- the r bits of the final cipher text are moved to the right-most r bits of the Shift Register and its r left-most bits are discarded.
- $C_i = E_k(C_{i-1}) \oplus P_i$; $P_i = E_k(C_{i-1}) \oplus C_i$; $C_0 = IV$

Cryptographic modes

Cipher FeedBack (CFB)



Cipher Feedback (CFB) mode Encryption



Cipher Feedback (CFB) mode Decryption

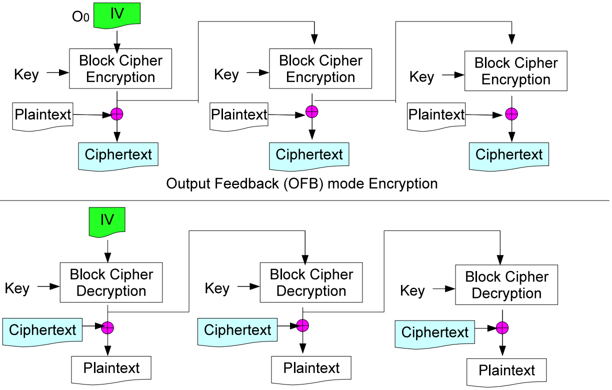
Cryptographic modes

Output FeedBack (OFB)

- plain text is encrypted in blocks of size r ($r < n$);
- the n-bit Shift Register (initially IV) is encrypted into an intermediate cipher text;
- the left-most r bits of the intermediate encrypted text are XORed with the next r bits of the plain text to obtain r bits of cipher text;
- the r bits of the intermediate cipher text are moved to the right-most r bits of the Shift Register and its r left-most bits are discarded
- $C_i = P_i \oplus O_i$; $P_i = C_i \oplus O_i$; $O_i = E_k(O_{i-1})$; $O_0 = IV$

Cryptographic modes

Output FeedBack (OFB)



Output Feedback (OFB) mode Encryption

Output Feedback (OFB) mode Decryption

Outline

Summary

Cryptography: basics

- Cryptography definitions and goals and terminologies
- Classical ciphers: substitution, transposition, and product cipher.
- Cryptographic modes: ECB, CBC, CFB, OFB
- Block cipher and stream cipher

Next lecture

- Number revision
- Block cipher and the Feistel structure
- Symmetric key encryption: DES in details