



BÀI THỰC HÀNH SỐ 1

Môn: MẬT MÃ & AN NINH MẠNG

-00o-

I. MỤC TIÊU

- Cung cấp kiến thức về các hệ mã đối xứng truyền thông
- Phương pháp phân tích mã trên các hệ mã đối xứng truyền thông
- Cách thức hoạt động của chuẩn mã hoá dữ liệu DES

II. CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH

Sinh viên ôn tập lại phần lý thuyết chương 1 và chương 2

III. CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI

- Sinh viên trả lời tất cả các câu hỏi trong bài thực hành vào file <MSV>_Lab01.docx (sử dụng mẫu file trả lời được đính kèm) và nộp bài theo deadline của bài Lab01 ở Bkel, không nhận bài nộp qua email hay các hình thức khác.
- Thời gian để thực hiện bài Lab là 14 ngày.

IV. NỘI DUNG THỰC HIỆN

Phần 1. Các hệ mã đối xứng truyền thông

1.1. Tham khảo một số hệ mã đối xứng truyền thông (cố điển)

a) Caesar Ciphers

Mật mã Caesar là một trong những kỹ thuật mã hóa đơn giản và phổ biến, là một dạng mật mã thay thế, trong đó mỗi ký tự trên văn bản sẽ được thay bằng một ký tự khác, có vị trí cách nó một khoảng xác định trong bảng chữ cái.

Ví dụ về mật mã Caesar thay thế mỗi ký tự trong bản rõ bằng một ký tự khác cách nó 3 ký tự trong bảng chữ cái ($k = 3$):

Position	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	26
Alphabets	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
3-posi-shift	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

Plaintext	Plaintext-arranged	Final ciphertext
MY EXAM IS EASY		PB HADP LV HDVB
I VISIT THE SCHOOL EVENT		L YLVLW WKH VFKRRO HYHQW
I LOVE EATING ICE-CREAM		L ORYH HDWLQJ LFHFUHDP

b) Vigenere Ciphers

Mật mã Vigenere là sự kết hợp xen kẽ vài phép mã hóa Caesar với các bước dịch khác nhau dựa trên khoá



Ví dụ:

Plaintext	keyword	Final ciphertext
MY EXAM IS EASY	ITALY	VS FJZV CT QZBS
I VISIT THE SCHOOL EVENT	LONDON	U KWWXH FWS WRVADZ IKSZI
I LOVE EATING ICE-CREAM	PARIS	Y MGEX UBLRGW JUN-VHFSV

c) Transposition Cipher

Mã chuyển vị là hình thức mã hóa mà các ký tự trong thông điệp ban đầu được hoán đổi vị trí cho nhau

Ví dụ về mã hoán vị đối với bản rõ (plaintext) là chuỗi bit nhị phân (binary):

Key Pattern: Key pattern: 1->4, 2->8, 3->1, 4->5, 5->7, 6->2, 7->6, 8->3			
Bit locations	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Plaintext(Binary)	0 0 1 0 0 1 0 1	0 1 1 0 1 0 1 1	0 0 1 1 0 1 1 1
Ciphertext	0 1 0 0 0 0 1 1	0 1 0 1 1 1 0 1	1 1 0 0 1 0 1 1
Bit location	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8

Ví dụ về mã hoán vị đối với bản rõ (plaintext) là chuỗi các ký tự alphabet:

"BOOK OR RUNNING KEY CIPHER"			
Key Pattern: Key pattern: 1->4, 2->8, 3->1, 4->5, 5->7, 6->2, 7->6, 8->3			
Letter locations	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Plaintext(letters)	B O O K O R R U	N N I N G K E Y	C I P H E R B O
Ciphertext	K U B O R O R O	N Y N G E N K I	H O C E B I R P
Bit location	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8

d) One-time Pad

Mật mã One-time Pad, hay còn được gọi là Vernam Cipher, tương tự mật mã Vigenere nhưng sử dụng khoá có độ dài bằng với độ dài văn bản được mã hoá, khoá được sinh ra ngẫu nhiên.

Ví dụ sử dụng One-time Pad để mã hoá plaintext: BOOK OR RUNNING KEY CIPHER

Plaintext	B	O	O	K	O	R	R	U	N	N	N	G	K	E	Y	C	I	P	H	E	R	
Plaintext value	2	15	15	11	15	18	18	21	14	14	9	14	7	11	5	25	3	9	16	8	5	18
One-time pad text	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A
One-time pad value	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
Sum of plaintext and pads	3	17	18	12	17	21	19	23	17	15	11	17	8	13	8	26	5	12	17	10	8	19
After Modulo subtraction																						
Ciphertext	C	Q	R	L	Q	U	S	W	Q	O	K	Q	H	M	H	Z	E	L	Q	J	H	S

Position	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	26
Alphabets	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



e) Mật mã Playfair

Mật mã Playfair sử dụng một ma trận chữ cái 5×5 được xây dựng từ khóa: điền các chữ cái của từ khóa vào ma trận khoá 5×5 theo thứ tự từ trái qua phải, từ trên xuống dưới (bỏ các chữ trùng), sau đó điền những vị trí còn lại của ma trận với các chữ cái khác của bảng chữ cái theo thứ tự alphabet, trong đó ký tự I, J ở trên cùng một ô của ma trận.

Ví dụ ma trận khoá với từ khoá 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

Thực hiện mã hoá từng 2 ký tự trên bản rõ dựa vào ma trận khoá theo quy luật như sau:

- Nếu 2 chữ cái giống nhau, tách ra bởi 1 chữ điền thêm (thường là X)
Ví dụ: EE sẽ được thay bởi EX
- Nếu 2 chữ cái nằm cùng hàng, thay bởi các chữ bên phải
Ví dụ: EF sẽ thay bằng FG
- Nếu 2 chữ cái nằm cùng cột, thay bởi các chữ bên dưới
Ví dụ: OF thay bằng HP
- Các trường hợp khác, mỗi chữ cái được thay bởi chữ cái khác cùng hàng, trên cột chữ cái cùng cặp
Ví dụ: ET sẽ thay bằng KL

1.2. Bài tập

Câu 1. Cho một bản mã (ciphertext) được tạo ra bằng cách dùng hệ mã Caesar để mã hoá một văn bản viết bằng tiếng Anh, hãy giải mã ciphertext trên mà không cần biết thông tin khoá và giải thích cách làm, từ đó cho biết điểm yếu của giải thuật Caesar là gì?

KNXMNSLKWXJXMBFYJWGJSIXFIRNYXB
TWIKNXMWFSITAJWMJQRNSLFSDIFD

Trợ giúp: sử dụng tần suất xuất hiện của các chữ cái trong các văn bản tiếng Anh cho trong bảng bên dưới để phân tích mã:

Table 1:

a	b	c	d	e	f	g	h	i	j	k	l	m
8, 05	1, 62	3, 2	3, 65	12, 31	2, 28	1, 61	5, 14	7, 18	0, 1	0, 52	4, 03	2, 25
n	o	p	q	r	s	t	u	v	w	x	y	z
7, 19	7, 94	2, 29	0, 20	6, 03	6, 59	9, 59	3, 1	0, 93	2, 03	0, 2	1, 88	0, 09



Câu 2. Cho ciphertext: **asvphgyt** đã được mã hoá bằng hệ mã thay thế theo công thức:

$$C = (M + K) \bmod 26$$

Trong đó C là bản mã (ciphertext), M là thông điệp (plaintext), K là khoá

Hãy tìm lại khoá K và giải mã thông điệp?

Câu 3. Cho một bản mã (ciphertext) được tạo ra bởi mật mã Affine với công thức như sau (bản rõ là một văn bản tiếng Anh):

$$C = E([a, b], p) = (ap+b) \bmod 26$$

Người ta nhận thấy rằng trong bản mã này, ký tự **B** xuất hiện nhiều nhất, ký tự **U** xuất hiện nhiều thứ hai, hãy tìm ra công thức đúng của hệ mã Affine nói trên (tìm giá trị a,b)?

Câu 4. Hãy nêu ra hai vấn đề đối với Mật mã One-time Pad?

Câu 5. Hãy sử dụng mật mã Playfair để mã hoá thông điệp bên dưới:

Must see you over Cadogan West. Coming at once.

Với ma trận khoá được sử dụng là:

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

Câu 6. Sử dụng mật mã Double Transposition (Tham khảo:

<https://www.pbs.org/wgbh/nova/decoding/doubtrans.html>), để mã hoá thông điệp bên dưới, mô tả từng bước thực hiện?

spyarrivesonthursday

Yêu cầu: sử dụng tên đệm để làm key1, và tên làm key2 (Ví dụ: sinh viên có tên Nguyễn Văn An thì key1=VAN, key2=AN).

Câu 7. SOLVE A CIPHER game. Truy cập vào trang web American Cryptogram Association bên dưới:

<http://www.cryptogram.org/resource-area/solve-a-cipher/>

Chọn “New Puzzle” và nhấn nút **Go!**, hãy sử dụng gợi ý và các công cụ trên trang web để tìm lại bản rõ (plaintext) từ bản mã (ciphertext) được tạo ra, ghi lại kết quả và giải thích cách làm, chụp ảnh màn hình kết quả?

Phần 2. Chuẩn mã hoá dữ liệu DES

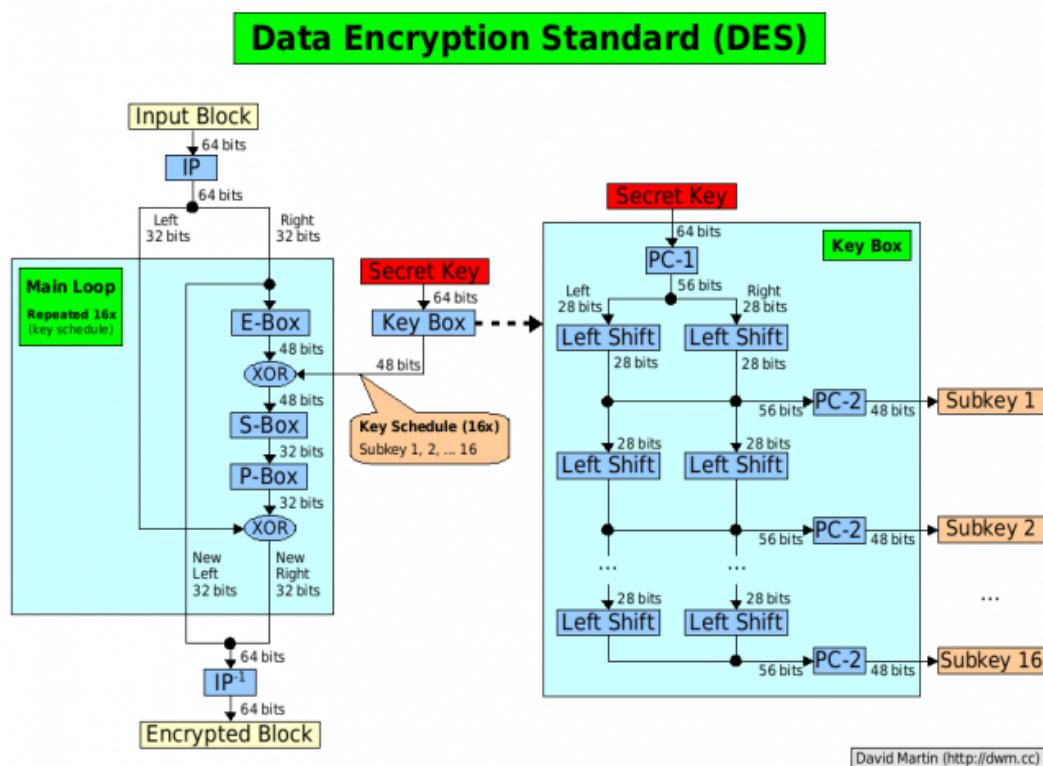
1.1. Giới thiệu chuẩn mã hoá dữ liệu DES

DES được công nhận vào năm 1977 bởi Viện nghiên cứu quốc gia về chuẩn của Mỹ (NIST – National Institut of Standards and Technology)

Nguyên lý hoạt động:

- Sử dụng một khóa K tạo ra n khóa con K1, K2, ..., Kn
- Hoán vị dữ liệu (Initial Permutation)
- Thực hiện n vòng lặp, ở mỗi vòng lặp:
 - + Chia dữ liệu thành 2 phần
 - + Áp dụng phép toán thay thế lên một phần (hàm F), phần còn lại giữ nguyên
 - + Hoán vị 2 phần cho nhau (trái \leftrightarrow phải)
- Hoán vị dữ liệu (Final Permutation)

Minh họa DES:



Ví dụ:

Ví dụ về cách thức hoạt động của giải thuật DES, sinh viên xem file đính kèm bài Lab (**Des-Example.pdf**)



1.2. Bài tập

Câu 1: Mô tả sự khác nhau giữa mã hoá khối và mã hoá dòng?

Câu 2: Sử dụng giải thuật mã hoá DES để mã hoá thông điệp theo thông tin và trả lời các câu hỏi như bên dưới (chỉ thực hiện mã hoá 1 vòng):

Thông điệp được cho dưới dạng Hex:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Khoa được cho dưới dạng Hex (với 4 ký tự cuối (**X**) là 4 số cuối của mã số sinh viên):

0	1	2	3	4	5	6	7	8	9	A	B	X	X	X	X
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Hãy trả lời các câu hỏi sau:

- a. Tính khoá con K1 được sử dụng cho vòng mã hoá đầu tiên
- b. Tính L0, R0
- c. Tính kết quả mở rộng R0: E[R0], với E là hàm mở rộng
- d. Tính giá trị A = E[R0] \oplus K1
- e. Chia 48-bit kết quả ở câu d và chia thành các nhóm 6 bit, thực hiện tính toán trên từng nhóm 6 bit thông qua S-box, ghi lại kết quả.
- f. Nối các kết quả tính được ở câu e thành chuỗi kết quả 32-bit, ghi lại kết quả dưới dạng binary (B).
- g. Tính giá trị P(B), với P là hàm hoán vị
- h. Tính giá trị R1 = P (B) \oplus L0
- i. Ghi lại kết quả ciphertext cho vòng thứ nhất