UNIVERSITY OF
Southampton
Electronics and Computer Science

Symmetric Cryptographic Systems

Revision Questions

Dr Basel Halak (bh9@ecs.soton.ac.uk)

Read the following statements carefully and explain whether or not they are correct:

✗ 1. Ciphers which adopt Feistel structure such as triple DES, must have an invertible round function otherwise decryption would be impossible.

$R_1, L_1 \rightarrow R_0\ L_0$

Possible $\rightarrow \begin{cases} R_1 = f(R_0) + L_0 \\ L_1 = R_0 \end{cases} \Rightarrow \begin{matrix} R_0 = L_1 \\ L_0 = R_1 - f(L_1) \end{matrix}$

↑ without invertible

→ only apply to cipher-only attack　　有弹性的

✗ 2. A cipher that satisfies Shannon perfect secrecy is resilient to chosen plaintext attacks.

Chosen plaintext attack → Access to number of plaintext and corresponding plaintext
Cipher plaintext attack → Access to only ciphertext

✗ 3. Rijndael cipher was adopted as the Advanced Encryption Standard (AES) in 2001, because it satisfies Shannon perfect secrecy.

✗ 4. ECB is the best cryptographic mode to use for encrypting images. identical patterns ← too many

→ only resilient to its algorithm

✗ 5. A semantically secure cipher is resilient to all side channel attacks.

✗ 6. In a counter mode block cipher, the loss of one encryption block will make it impossible to decipher the following encrypted blocks. If there is an error in C_1, it only affects P_1

✓ 7. A shift cipher is immune to a ciphertext only attack, if messages are only one letter long.

→ use cipher block ε generate another cipher block

✗ 8. The use of CBC cryptographic mode guarantees system security against known plaintext attack regardless of the length of the messages you encrypt using the same key

If get more equations → more information the attacker get　　advantage increases as the length increases using the same key
If the length is under a specific range

✓ 9. Although Double-DES is subject to a meet in the middle attacks, it is still a more secure system then DES. (meet-in-the-middle attack)　　安全一点点也是安全一点点

✓ 10. Compression techniques enhance the security of a cryptosystem by removing redundant information, hence making cryptanalysis harder.

Exercise 1: If $P=(-3,9)$ and $Q=(-2,8)$ on the elliptic curve $y^2=x^3-36x$, find $P+Q$ and $2P$

Find all points P such that $2P=0$

[P+Q] $\begin{cases} P=(-3,9)=(x_1,y_1) \\ Q=(-2,8)=(x_2,y_2) \end{cases} \Rightarrow \lambda=\frac{y_2-y_1}{x_2-x_1}=\frac{8-9}{-2-(-3)}=-1 \Rightarrow \begin{cases} x_R=\lambda^2-x_1-x_2=1+5=6 \\ y_R=-y_1+\lambda(x_1-x_R)=-9+(-1)(-3-6)=0 \end{cases} \Rightarrow P+Q=[6,0]$

[2P] $P=(-3,9)=(x_1,y_1) \Rightarrow \lambda=\frac{3x_1^2+a}{2y_1}=\frac{27-36}{18}=-\frac{1}{2} \Rightarrow \begin{cases} x_R=\lambda^2-2x_1=\frac{1}{4}+6=\frac{25}{4} \\ y_R=-y_1+\lambda(x_1-x_R)=-9-\frac{1}{2}(-3-\frac{25}{4})=-\frac{35}{8} \end{cases} \Rightarrow 2P=[\frac{25}{4},-\frac{35}{8}]$

[2P=0] $x^3-36x=0$

$x=0$

$x\neq 0$, $x^2-36=0$, $x=\pm 6$

(∞,∞)
$(0,0)$
$(6,0)$
$(-6,0)$

$[\mathbb{Z}_7]$ $1^2=1$, $2^2=4$, $3^2=2$, $4^2=2$, $5^2=4$, $6^2=1$

QR: $\{1,2,4\}$
±1 ±3 ±2
$\downarrow$ $\downarrow$ $\downarrow$
1,6 3,4 2,5

$[\mathbb{Z}_{11}]$ $1^2=1$ ✓, $2^2=4$ ✓, $3^2=9$ ✓, $4^2=5$ ✓, $5^2=3$ ✓, $6^2=3$ ✓, $7^2=5$ ✓, $8^2=9$ ✓, $9^2=4$ ✓, $10^2=1$ ✓

QR: $\{1,3,4,5,9\}$

Exercise 2: Find the quadratic residues in $\mathbb{Z}_7$ and $\mathbb{Z}_{11}$, together with their square roots.

if x in $(\mathbb{Z}_p)^*$ is a Q.R. then $x^{\frac{p-1}{2}}=1$ in $\mathbb{Z}_p$

Exercise 3: Let $F=\mathbb{Z}_5$. Find the orders of the elliptic curves $y^2=x^3-1$ and $y^2=x^3+x+1$

x	0	1	2	3	4
x^3-1	-1	0	7	26	63
x^3-1 in $\mathbb{Z}_5$	4	0	2	1	3
	2,3	0	X	1,4	X

$\Rightarrow$ Order $=2+1+0+2+0+1=6$

y	0	1	2	3	4
$(\mathbb{Z}_5)$ y^2	0	1	4	4	1

x	0	1	2	3	4
x^3+x+1	1	3	1	1	4
	1,4	X	1,4	1,4	2,3

y	0	1	2	3	4
y^2	0	1	4	4	1

$\Rightarrow$ Order $=2+0+2+2+2+1=9$

Exercise 4: Let E_1 and E_2 be the elliptic curves $y^2=x^3-x$ and $y^2=x^3-x+1$, with $F=\mathbb{Z}_5$.
Show that both have order 8. Show that E_1 is not cyclic, is E_2 cyclic?

$y^2=x^3-x$

x	0	1	2	3	4
x^3-x	0	0	1	4	0
	0	0	1,4	2,3	0
y	0	1	2	3	4
y^2	0	1	4	4	1

Order $=1+1+2+2+1+1=8$

$(0,0)$ $(1,0)$ $(4,0)$

$P=2 \rightarrow$ not cyclic
有3个点 $=P^2-1=3$

P
$\boxed{8=2\times2\times2}$

$(0,0)$
$(1,0)$
$(2,1)$
$(2,4)$
$(3,2)$
$(3,3)$

$(0,0)$
$(1,0)$
$(2,1)$ $(2,4)$
$(3,2)$ $(3,3)$
$(4,0)$

2 P^2-1 3

2

$y^2=x^3-x+1$

x	0	1	2	3	4
x^3-x+1	1	1	2	0	1
	1,4	1,4	X	0	1,4
y	0	1	2	3	4
y^2	0	1	4	4	1

order $=2+2+0+1+2+1=8$

$(3,0) \Leftarrow P-1=1$

$P=2 \rightarrow$ cyclic 了

所在 $<P^2-1=3$

$\Downarrow$

Only one of them is order 2

$(3,0)$ is the generator of $(3,0)$ & (∞,∞)

$3,0+3,0$ (

2

2×5

Exercise 5: Let E be the elliptic curve $y^2=x^3+x+6$ over $F=\mathbb{Z}_{11}$.
Show that $|E|=13$. Taking $P=(2,7)$ as a generator, find an integer i such that $iP=(8,8)$ in E

x	$y^2=$	
0	6	X
1	8	X
2	5=16	4,7
3	3=25	5,6
4	8	X
5	4	2,9
6	8	X
7	4	2,9
8	9	3,8
9	7	X
10	4	2,9

order $=2\times6+1=13$

1P (2,7)
2P (5,2)
3P (8,3)
4P (10,2)
5P (3,6)
6P (7,9)
7P (7,2)
8P (3,5)
9P (10,9)
10P (8,8) ←
11P (5,9)
12P (2,4)

2