Name Surname: ____________________ **Student #:____________**

CENG 471 CRYPTOGRAPHY
Midterm-1 Exam, 23 March 2018 Q&A

Exam duration is two hours.

Q.1 (30 points)

a) **(10 points)** How can symmetric algorithms such as DES be made more secure please justify your opinions?

Answer: Theoretically, there are two ways" either the key length needs to be increased, or the number of rounds in the encryption process needs to be increased. Both of these solutions tend to increase the processing power required to encrypt and decrypt data and slow down the encryption/decryption speed, because of the increased number of mathematical operations required. Examples of modified DES include Triple Data Encryption Standard (3DES) and DESX)

b) **(10 points)** Please explain the following terms: “avalange affect”, “diffusion”, “confusion”.

Answer: In symmetrical crypto-systems such as in DES and AES; effect of one-bit difference on key or plaintext does affect approximately %50 bits of encrypted block, which is called avalange affect.

“Diffusion” term defines the expected high complexity between plaintext and ciphertext from the view of attacker.

“Confusion” term defines the expected high complexity between key and ciphertext from the view of attacker.

c) **(10 points)** Please explain that what is the structure of Fiestel structure and difference between Lucifer and DES?

Answer: In DES (Data Encryption Standard) uses Fiestel Structure of Lucifer which was invented by Horst Fiestel. He used Substitution-Permutation (S-P) Network structure which is proposed by Shannon 1949. In Fiestel structure, diffusion is achieved by permutations and confusion is achieved by XOR operations. The Lucifer works on 64 bits data blocks with 128bit key. But in DES, 64bit data blocks are enc/decrypted by 64 bit key.

Q.2 (20 points) Let $E_k(m), D_k(c)$ be a block cipher. Fischer Spiffy Mixer (FSM) mode encrypts a sequence of message blocks $m_1, m_2, \ldots$, by the sequence of ciphertext blocks $c_1, c_2, \ldots$, using the following method:

$$c_i = m_{i-1} \oplus E_k(m_i \oplus c_{i-1}), i \geq 1$$

m_0 *and* c_0 are fixed (public) initialization vectors.

a) Describe how decryption is performed.

b) Suppose ciphertext block c_i is damaged in transit. Which plaintext blocks become undecipherable as a result? Explain why?

Answer:

a) XORing m_{i-1} to both sides of the encryption equation gives

$c_i \oplus m_{i-1} = E_k(m_i \oplus c_{i-1})$

Name Surname: ____________________ **Student #:____________**

CENG 471 CRYPTOGRAPHY
Midterm-1 Exam, 23 March 2018 Q&A

Exam duration is two hours.

Applying the decryption function on both sides gives:
$D_k(c_i \oplus m_{i-1}) = m_i \oplus c_{i-1},\ so \quad m_i = c_{i-1} \oplus D_k(c_i \oplus m_{i-1}).$

b) If c_i was damaged then m_i is damaged. If m_i is damaged then m_{i+1} is damaged. From then on all messages are damaged.

Q.3 (20 points) In the course, the four basic modes of operations of block ciphers (ECB, CBC, CFB, OFB) are analyzed with respect to error propagation in encryption.

ECB: uses $C_i = E_K(P_i)$	CBC: uses $C_{-1} = IV$ $C_i = E_K(P_i \text{ XOR } C_{i-1})$
CFB: uses $C_{-1} = IV$ $C_i = P_i \text{ XOR } E_K(C_{i-1})$	OFB: uses $C_i=P_i \text{ XOR } E_K(O_{i-1})$, with $O_{-1}=IV$

In your answer, for all of four modes of operation; Please analyze the effect of erroneously received block $c_j,\ 1 \leq j < n$ on the decryption of remaining blocks. That is, specify which of plaintext blocks $x_j, x_{j+1}, x_{j+2}, \dots, x_n$ are received correctly by receiver.

Answer:

- ECB- Electronic Code Book mode: Message is broken into independent blocks which are encrypted, therefore only x_1 decrypted incorrectly.
- CBC-Cypher Block Chain mode: here each of previous cipher blocks is chained with current plaintext block, so a cipher text block depends on all blocks before it, therefore this erroneous ciphertext block c_j affects the description of following packets and their results as $x_j, x_{j+1}, x_{j+2}, \dots, x_n$.
- CFB-Cypher Feedback mode: Message block length can be 1,8,64 or 128 bit and denoted CFB-1, CFB-8 or CFB-64 etc. Errors during transmission of c_j propagate only x_j, x_{j+1} decrypted incorrectly
- OFB-Output Feedback mode: Errors do not propagate with this scheme. Only x_j is decrypted incorrectly.

Q.4 (20 points)

a) The so called S-box (Substitution box) is widely used cryptographic primitive in symmetric-key cryptosystems. In AES (Advanced Encryption Standard) the 16 S-boxes in each round are identical. All these S-boxes implement the inverse function in the Galois Field GF(2^8), which can also be seen as a mapping, $S: \{0,1\}^8 \rightarrow \{0,1\}^8$, so that

$$x \in GF(2^8) \overset{S}{\rightarrow} x^{-1} \in GF(2^8),$$

that is 8 input bits are mapped to 8 output bits. What is the total number of possible mappings one can specify for function S ?

Hint: Any function $f: GF(2^n) \rightarrow GF(2^n)$ can be represented as a polynomial,

Name Surname: ____________________ **Student #:**____________

CENG 471 CRYPTOGRAPHY
Midterm-1 Exam, 23 March 2018 Q&A

Exam duration is two hours.

$$f(x) = a_0 + a_1(x) + a_2x^2 + \cdots + a_{2^n-2}.x^{2^n-1} + a_{2^n-1}.x^{2^n-1}, a_i \in GF(2^n)$$

b) Construct the Galois field of 16 elements, $GF(2^4)$, using a primitive polynomial $f(x) = x^4 + x + 1$.
Compute the powers $x^i, 0 \leq i \leq 14$ and represent these powers (multiplicative group) as polynomials of the form $a_0 + a_1x + a_2x^2 + a_3x^3$.

Answer

a) The question is how many mappings are there over the field $GF(2^n)$. Using the hint any function $f: GF(2^n) \to GF(2^n)$ can be represented as a polynomial,

$$f(x) = a_0 + a_1(x) + a_2x^2 + \cdots + a_{2^n-2}.x^{2^n-1} + a_{2^n-1}.x^{2^n-1}, a_i \in GF(2^n)$$

Any a_i can be chosen in 2^n ways, the total number of mappings over $GF(2^n)$ is,
$2^n2^n2^n \ldots 2^n = (2^n \; times \; 2^n) = 2^{n2^n}$.

b) In our course, the field of 8 elements $GF(2^3)$ is constructed. We use the primitive polynomial $x^4 + x + 1$:

$\boldsymbol{x^i}$	$\boldsymbol{a_3a_2a_1a_0}$
0	0000
$\boldsymbol{x^0}$	**0001**
x^1	0010
x^2	0100
x^3	1000
$x^4 = x + 1 \; (mod \; x^4 + x + 1)$	0011
$x^5 = x.x^4 = x^2 + x \; (mod \; x^4 + x + 1)$	0110
.	.
.	.
.	.
$x^{14} = x^3 + 1$	1001
$\boldsymbol{x^{15} = x^4 + x = 1}$	**0001**

Q.5 (10 points) Encrypt the message, “the king is in grave danger” using the Vigenere Cipher with the keyword **“HISMAJESTY”.**

Answer:

t h e k i n g i s i n g r a v e d a n g e r

h i s m a j es t y h i s m a j e s t y h i

---

a p w w i w k a l g u o j m v n h s g e l z