Cryptographic Algorithms and Protocols
Exercise A (2023)

Student Name:____________________ **Student No.:_______________**

Question No.	I	II	III	IV	V	Total Score
Score						

I. Blank Filling (Please write the answer above the line.)

1) Suppose Bob receives a ciphertext **ZHZLOOPHHWDWPLGQLJKW** that is generated by the Caesar Cipher. Then the plaintext is__we will meet at midnight___.
2) DES and AES are two block ciphers. DES has block length _64_bits, and key length_56 bits. AES has block length_128__bits, and three allowable key lengths:_128__bits,_192 bits and__256__bits.
3) Different from the SHA-1 that was designed by the Merkle-Damgard construction, SHA-3 is based on the design strategy called____the sponge construction____, which can produce a message digest of arbitrary length.
4) Please list at least four different substitution ciphers: __the Shift Cipher, _the Caesar Cipher, the Affine Cipher, ____the Vigenere Cipher, ___the Hill Cipher__.
5) It is recommended that the message digest of a secure hash function is 224 bits since the birthday attack requires ____2^{112}_____steps.
6) Suppose that π is a permutation of {1, 2, 3, 4, 5, 6, 7, 8} as follows:

x	1	2	3	4	5	6	7	8
$\pi(x)$	2	5	1	8	3	7	4	6

Then the inverse of this permutation π is:_______________

y	1	2	3	4	5	6	7	8
$\pi^{-1}(y)$	3	1	5	7	2	8	6	4

II. Multiple Choice (Please choose the correct answer for each question.)

1) The number of all different permutations of $\{1,2,\cdots,n\}$ is (C).
   A. n B. n^2 C. $n!$ D. $\log n$
2) Which attack model in the following is usually considered to be the weakest one? (A).
   A. ciphertext only attack B. known plaintext attack
   C. chosen plaintext attack D. chosen ciphertext attack
3) There are four modes of operation developed for DES and standardized in FIPS Publication

81 in 1980. The four modes did not include (B).

A. electronic codebook mode (ECB) B. counter mode

C. cipher feedback mode (CFB) D. output feedback mode (OFB)

4) The Secure Hash Algorithm SHA-1 is an iterated hash function, whose message digest has__B___bits.

A. 128 B. 160 C. 224 D. 256

5) The number of positive integers that are smaller than n and relatively prime to n is called Euler phi-function of n and denoted by $\phi(n)$. If an integer a is relatively prime to n, then the multiplicative inverse, i.e., a^{-1}mod n exists. What are the value of $\phi(26)$ and 3^{-1}mod26, respectively? (A)

A. 12, 9 B. 12, 13 C. 10, 9 D. 10, 13

6) Shannon proved the unconditionally security of the One-Time Pad in 1949. Which of the following descriptions for the One-Time Pad is wrong? (D)

A. The One-time Pad provides perfect secrecy.

B. Each key of the One-Time Pad is used for only one encryption.

C. The One-Time Pad is vulnerable to a known-plaintext attack since the key k can be computed easily.

D. The amount of key is smaller than the amount of plaintext.

7) Among the following Secure Hash Algorithms, which is adopted as a standard by NIST on August 5, 2015. (C)

A. SHA-1 B. SHA-256 C. SHA-3 D. SHA-0

8) Among the following MACs, which is based on hash functions and adopted as a standard by NIST on 2002. (B)

A. DDA B. HMAC C. CBC-MAC D. CMAC

9) Which of the following ciphers is a mechanical cipher and was widely used in World War II? (C)

A. Spartan Scytale Cipher B. Caesar Cipher

C. Enigma D. Bombe

10) Stream Ciphers have been used in many applications. Among the following descriptions, which is not a practical stream cipher? (A)

A. LFSR used in keystream generation

B. CSS (Content Scramble System) used in DVD encryption

C. A5 used in GSM encryption

D. E0 used in Bluetooth encryption

E. RC4 used in HTTPS

III. True-False (Please determine the truth of each description.)

1) The Shift Cipher is a kind of Symmetric Cryptosystem. (T)

2) The Kerckhoffs' Principle says that the opponent knows the cryptosystem being use. (T)

3) Let y=DES(x,K) represent the encryption of plaintext x with key K using the DES cryptosystem, and c[•] denote the bitwise complement of its argument. Then c[y]=DES(c[x],c[K]) . (T)

4) Message authentication codes are unkeyed hash functions. (F)

5) A Las Vegas algorithm is a randomized algorithm which may fail to give an answer, but if the algorithm does return an answer, then the answer must be correct. (T)

6) The cryptographic tools that help to achieve integrity of data include Message Authentication Codes (MACs), Signature Schemes and Hash Functions. (T)

7) Different from the MD4, MD5, SHA-0, SHA-1 that were designed by the Merkle-Damgard construction, SHA-2 was designed by the sponge construction, which can produce a message digest of arbitrary length. (F)

8) DES is the first encryption standard in the world that is a block cipher and was developed in 1970s. In DES, the design of S-boxes that is the sole non-linear component is vital to the security since it introduce difficulties in linear cryptanalysis and differential cryptanalysis. (T)

9) The S-box in AES can not only be represented by a 16 by 16 array, but also can be defined algebraically by introducing the concept of finite field, which provides security against differential and linear attacks. (T)

10) Most modern block ciphers are designed iteratively and incorporate the substitution-permutation network (SPN). DES is such an iterated cipher with 10 rounds encryptions. (F)

11) The conditional entropy H(K|C), called the key equivocation, is a measure of the amount of uncertainty of the key remaining when the plaintext is known. (F)

IV. Answer Questions.

1) Consider the Affine Cipher over Z_{55}. Suppose that $k = (7, 16)$ is a key in the Affine Cipher. Express the decryption function $d_k(y)$ in the form $d_k(y) = a'y + b'$, where $a', b' \in Z_{55}$.

Answer: The encryption rule of the considered Affine Cipher is

$y=e_K(x) = ax + b = 7x+16 \pmod{55}$

i) $a' = a^{-1} \bmod 55 = 7^{-1} \bmod 55 = 8$ as $7*8=1 \pmod{55}$ (3º)

ii) As the plaintext x itself should be obtained after decryption, we have

$$
\begin{aligned}
x &= d_K(y) \\
&= d_K(e_K(x)) \\
&= a'(7x+16) + b' \pmod{55} \\
&= 8(7x+16) + b' \pmod{55} \\
&= (x+18 + b') \pmod{55}
\end{aligned}
$$

Therefore, $b' = 37$ (6º)

Hence, the decryption function is $d_K(y) = (8y + 37) \pmod{55}$. (1º)

2) Prove that the Affine Cipher over Z_{55} as given in the above problem, i.e.,

$$y=e_K(x) = ax + b = 7x+16 \pmod{55}$$

achieves perfect secrecy if every key is used with equal probability 1/2200.

Answer: The encryption rule of the considered Affine Cipher is

$$y=e_K(x) = ax + b = 7x+16 \pmod{55}$$

The keyspace K is

$$K = \{k=(a, b) \in Z_{55} \times Z_{55}: \gcd(a, 55) =1\}.$$

So the size of the keyspace is $|K|=\phi(55)*55 = 40*55=2200$. (2º)

If every key is used with equal probability 1/2200, then for any x, y in Z_{55},

$$p(y \mid x) = \sum_{\{k=(a,b) \mid x=d_k(y)\}} p(k) = \sum_{\{a \mid a \in Z_{55}^*\}} 1/2200 = 40/2200 = 1/55, \quad (3^o)$$

as if x, y and a are given, then b=y-ax (mod 55) is determined.
Moreover, for any y in Z_{55},

$$p(y) = \sum_{x \in Z_{55}} p(x) p(y \mid x) = 1/55 \sum_{x \in Z_{55}} p(x) = 1/55 \quad (3^o)$$

Then

$$\mathrm{p(x|y)} = \frac{\mathrm{p(x)p(y|x)}}{\mathrm{p(y)}} = \mathrm{p(x)},$$

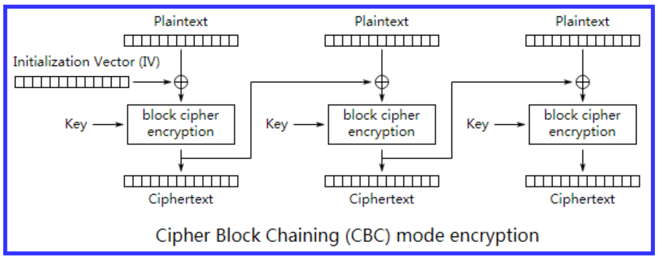
which proves the perfect secrecy. (2^o)

3) To encrypt long sequences by Block Ciphers, different modes of operation have been developed. What are the CBC mode and the OFB mode? Please show main differences between these two modes.

Answers: In CBC mode, each ciphertext block y_i is x-ored with the next plaintext block, x_{i+1}, before being encrypted with the key:

Encryption (figure)

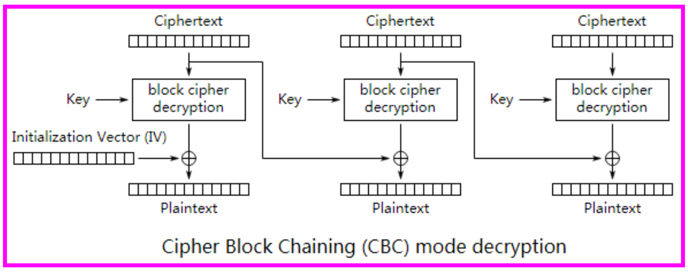
$$y_0 = \mathrm{IV}$$
$$y_i = e_K(y_{i-1} \oplus x_i)$$



Cipher Block Chaining (CBC) mode encryption

Decryption (figure)

$$y_0 = \mathrm{IV}$$
$$x_i = y_{i-1} \oplus d_K(y_i)$$

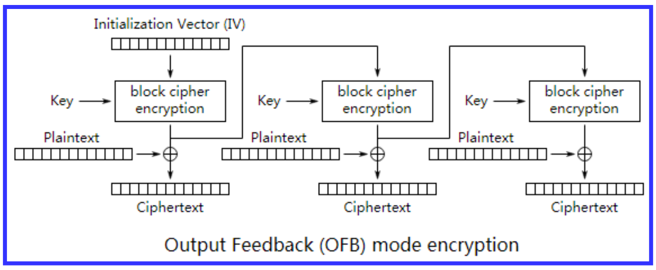


Cipher Block Chaining (CBC) mode decryption

In OFB mode, a keystream is generated, which is then x-ored with the plaintext:

Encryption (figure)

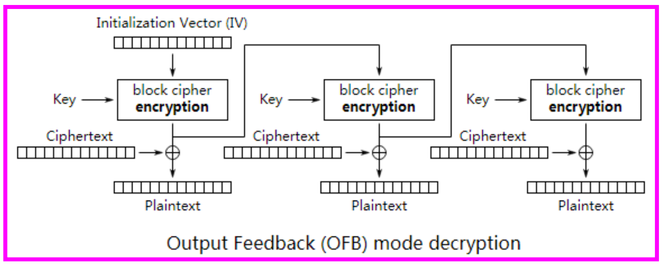
$$z_0 = \mathrm{IV}$$
$$z_i = e_K(z_{i-1})$$
$$y_i = x_i \oplus z_i$$



Output Feedback (OFB) mode encryption

Decryption (figure)

$$z_0 = \mathrm{IV}$$
$$z_i = e_K(z_{i-1})$$
$$x_i = y_i \oplus z_i$$



Output Feedback (OFB) mode decryption

One main difference is that: the encryption function is used for both encryption and decryption in OFB mode.

4) Suppose g is a collision resistant hash function that takes an arbitrary bitstring as input and produces an n-bit message digest. Define a hash function h as follows:

$$h(x) = \begin{cases} 0 \| x, & \text{if } x \text{ is a bitstring of length } n, \\ 1 \| g(x), & \text{otherwise.} \end{cases}$$

(a) Prove that h is collision resistant.

(b) Prove that h is not preimage resistant. More precisely, show that preimages (for the function h) can easily be found for half of the possible message digests.

Answer:

(a) Proof: ~~Suppose~~ h is not collision resistant,

~~then~~ Suppose $\exists\, z_1 \neq z_2$ s.t. $h(z_1) = h(z_2)$

i) If $len(z_1) \neq n$, & $len(z_2) \neq n$.

then $h(z_1) = 1 \| g(z_1) = 1 \| g(z_2) = h(z_2)$

$\Rightarrow g(z_1) = g(z_2)$ contradiction with that g is collision resistant.

ii) If $len(z_1) = n$ & $len(z_2) \neq n$

then $h(z_1) = 0 \| z_1 \neq 1 \| g(z_2) = h(z_2)$. This case doesn't happen.

iii) If $len(z_1) = n$ & $len(z_2) = n$

then $h(z_1) = 0 \| z_1 \neq 0 \| z_2 = h(z_2)$ since $z_1 \neq z_2$. This case doesn't happen.

$\therefore$ h is collision resistant.

(b) proof: For the image y where $y = (0, y_2, y_3 \cdots y_{n+1})$,

~~the preimage~~ Let $z = (y_2, y_3 \cdots y_{n+1})$. Then $len(z) = n$.

z is the preimage of y because ~~since~~ $h(z) = 0 \| z = y$.

$\therefore$ h is not preimage resistant.

5) Suppose the current State of 128 bits is

3243F68885A308D313198A250307734A

Please write the above State in a 4 by 4 square array, and the new State after the substitution using the following AES S-box.

Table 1: The AES S-box.

	Y															
X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Answer:

The State is

32	85	13	03
43	A3	19	07
F6	08	8A	73
88	D3	25	4A

After the substitution using the above AES S-box, the State becomes

23	97	7D	7B
1A	0A	D4	C5
42	30	7E	8F
C4	66	3F	D6

6) Suppose that $f:\{0,1\}^m \to \{0,1\}^m$ is a preimage resistant bijection. Define the function as follows

$$h:\{0,1\}^{2m} \to \{0,1\}^m$$
$$h(x) = f(x' \oplus x'')$$

where $x \in \{0,1\}^{2m}$ is represented as $x = x' \,||\, x''$ and $x', x'' \in \{0,1\}^m$.

Prove that the function h is not second preimage resistant.

Answer:

Let $x_1=x'||x''$, $x' \neq x''$ and $x', x'' \in \{0,1\}^m$. Denote $y= h(x_1)$

Set $x_2=x''||x'$.

Then $x_1 \neq x_2$, but $h(x_1) = f(x' \oplus x'')=f(x'' \oplus x')=h(x_2)$.