Cryptographic Algorithms and Protocols
Exercise A (2022)

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_____.
2) DES and AES are two block ciphers. DES has block length_____bits, and key length _____bits. AES has block length_____bits, and three allowable key lengths:_____bits, _____bits and_____bits.
3) Different from the SHA-1 that was designed by the Merkle-Damgard construction, SHA-3 is based on the design strategy called_____, which can produce a message digest of arbitrary length.
4) Please list at least four different substitution ciphers: _____.
5) It is recommended that the message digest of a secure hash function is 224 bits since the birthday attack requires _____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:_____.

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

1) The number of all different permutations of $\{1,2,\cdots,n\}$ is ( ).
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. 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 ( ).
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_____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., $a^{-1} \bmod n$ exists. What are the value of $\phi(26)$ and $3^{-1} \bmod 26$, respectively? ( )

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? ( )

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. ( )

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. ( )

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? ( )

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. 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. ( )

2) The Kerckhoffs' Principle says that the opponent knows the cryptosystem being use. ( )

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]) . ( )

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

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. ( )

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

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 $a', b' \in Z_{55}$.

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.

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.

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.

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

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.