Cryptographic Algorithms and Protocols - Exercise A (2024)

Student Name:_____ **Student No.:**_____

I. Blank Filling (Please write the answer above the line. 18%)

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. (how many are their rounds?)
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) It is recommended that the message digest of a secure hash function is 224 bits since the birthday attack requires ____2^{112}_____steps.
5) The integer n = 101 * 113, then its Euler phi-function is $\phi(n)$ = 100*112=11200.
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. 20%)

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) 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.

6) 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

7) 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

8) 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

9) In World War II, the mechanical machine designed by the group led by Alan Turing to break Enigma is _____. (D)

A. the mouse called Theseus

B. The digital computer trainer called Minivac 601

C. Turing machine

D. Bombe

10) Suppose in the cryptosystem (P, C, K, E, D) each key is used for only one encryption. Define random variables P, K, C on the plaintext set P, the keyspace K and the cipehrtext set C, respectively. The conditional entropy H(K|C), called key equivocation, measures the amount of uncertainty of the key remaining when ciphertext is known. Among the following equalities, which one must be true? (C)

A. $H(K,C)=H(K)+H(C)$ B. $H(P,C)=H(P)+H(C)$

C. $H(K\mid C)=H(P)+H(K)-H(C)$ D. $H(P,K,C)=H(P)+H(K)+H(C)$

III. True-False (Please determine the truth of each description. 22%)

1) A hash function is considered to be secure if the three problems of Preimage, Second Preimage and Collision are difficult to solve. (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) 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)

7) 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)
8) 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)
9) Suppose Oscar tries to determine the key of the cryptosystem to break it under the ciphertext-only attack model. After Oscar rules out certain keys, there are still many remaining possible keys, among which only one is the correct key and others are the incorrect keys called spurious keys. The unicity distance of the cryptosystem is defined to be the average amount of ciphertexts at which the expected number of spurious keys becomes zero (i.e., at which an opponent is able to uniquely compute the key) given enough computing time. (T)
10) Stream Cipher, Vigenere Cipher and Hill Cipher are all polyalphabetic cryptosystems. (F)
11) Suppose a synchronous stream cipher has the keystream generator g as:

$$g: \quad z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2, \quad i \geq 1.$$

Then for each of the 16 possible initialization vectors (z_1, z_2, z_3, z_4), the period of the resulting keystream is 5. (F)

IV. Answer Questions. 40%

1) (10%) Consider the Affine Cipher over Z_{26}. Suppose that $k = (3, 14)$ is a key in the Affine Cipher.
(1) Express the decryption function in the form $d_k(y) = a'y + b'$, where $a', b' \in Z_{26}$.
(2) Prove that this Affine Cipher achieves perfect secrecy if every key is used with equal probability 1/312.

Answer:

(1) The encryption rule of the considered Affine Cipher is

$y = e_K(x) = ax + b = 3x + 14 \pmod{26}$

i) $a' = a^{-1} \bmod 26 = 3^{-1} \bmod 26 = 9$ as $3*9 = 1 \pmod{26}$ (2^o)

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

$$\begin{aligned} x &= d_K(y) \\ &= d_K(e_K(x)) \\ &= a'(3x+14) + b' \pmod{26} \\ &= 9(3x+14) + b' \pmod{26} \\ &= (x + 22 + b') \pmod{26} \end{aligned}$$

Therefore, $b' = 4$ (2^o)

Hence, the decryption function is $d_K(y) = (9y + 4) \pmod{26}$. ($1^o$)

(2) The keyspace K is

$$K = \{k=(a, b) \in Z^*_{26} \times Z_{26}: \gcd(a, 26) = 1\}.$$

So the size of the keyspace is $|K| = \phi(26) * 26 = 12*26 = 312$.

If every key is used with equal probability 1/312, then for any x, y in Z_{26},

$$p(y \mid x) = \sum_{\{k=(a,b)|x=d_k(y)\}} p(k) = \sum_{\{a|a\in Z_{26}^*\}} 1/312 = 12/312 = 1/26 \ , \quad (2^o)$$

as if x, y and a are given, then b=y-ax (mod 26) is uniquely determined.
Moreover, for any y in Z_{26},

$$p(y) = \sum_{x\in Z_{26}} p(x)p(y \mid x) = 1/26 \sum_{x\in Z_{26}} p(x) = 1/26 \quad (2^o)$$

Then

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

which proves the perfect secrecy. (1^o)

2) (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.

X	Y															
	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

3) (5%) Suppose that X = (x_1, . . . , x_n) and X' = (x'_1, . . . , x'_n) are two sequences of n plaintext

blocks. Define

$$\text{same}(X, X') = \max\{j : x_i = x'_i \text{ for all } i \leqslant j\}.$$

Suppose X and X' are encrypted in CFB mode using the same key and the same IV. Show that it is easy for an adversary to compute same(X, X').

Answers:

For CFB mode, encryption and decryption are show as follows:

$$y_0 = \text{IV} \qquad y_0 = \text{IV}$$

$$z_i = e_K(y_{i-1}) \qquad z_i = e_K(y_{i-1})$$

$$y_i = x_i \oplus z_i \qquad x_i = y_i \oplus z_i$$

If the same key and the same IV are used, then it is easy to compute the following value from the ciphertexts Y and Y' as same(X, X') = same(Y, Y').

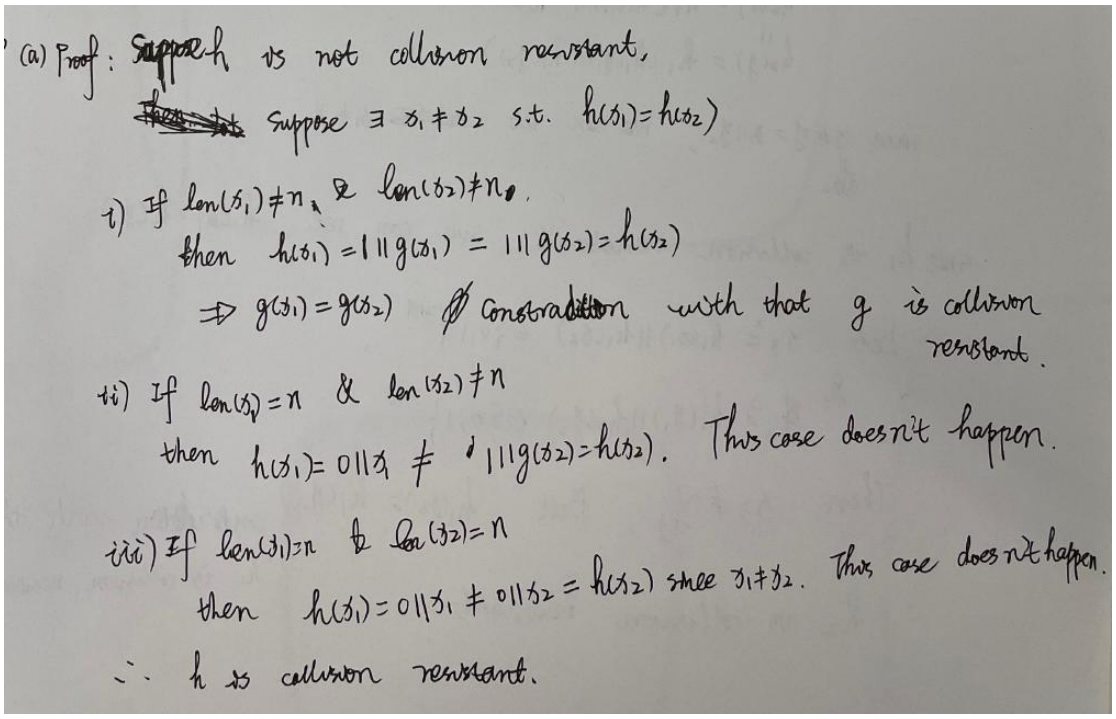
4) (10%) Suppose g is a collision resistant hash function that takes an arbitrary bitstring as input and produces an n-bit message digest. Define a hash function h as follows:

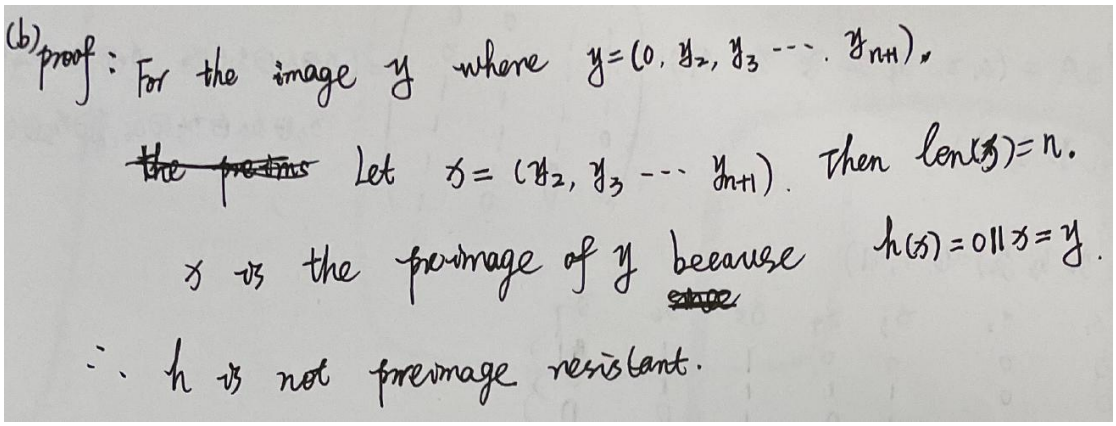
$$h(x) = \begin{cases} 0 \| x, & \text{if } x \text{ is a bitstring of length } n, \\ 1 \| g(x), & \text{otherwise.} \end{cases}$$

(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:





5) (10%) Suppose that (P, C, K, E, D) is a cryptosystem with $P = C = \{0, 1\}^m$. Let $n \geq 2$ be a fixed integer, and define a hash family (X, Y, K, H), where each hash function is a map from the set $X=(\{0, 1\}^m)^n$ to the set $Y=\{0, 1\}^m$, defined as follows:

$$h_k(x_1, \ldots, x_n) = e_k(x_1) \oplus \ldots \oplus e_k(x_n).$$

Suppose that $(x_1, \ldots, x_n)$ is an arbitrary message. Show how an adversary can then determine $h_k(x_1, \ldots, x_n)$ by using at most one oracle query. That is, there exists a **selective forgery** for this hash function.

Answer: