NUS CS-3235: Computer Security September 27, 2023

Quiz 1

Lecturer: Reza Shokri

Question 1. (5 pts).

Recall the definition of perfect secrecy in encryption: the adversary cannot gain any extra knowledge about a plaintext m, after observing its corresponding ciphertext c. Formally for any $m \in \mathcal{M}, c \in \mathcal{C}$, we can express this as

$$P(M = m|C = c) = P(M = m).$$

Under which of the following key distribution(s), the one-time pad encryption scheme (with $\mathcal{K} = \mathcal{M} = \{0,1\}^l$) achieves perfect secrecy? There could be multiple correct answers. (Let x^l represent a sequence of xs of length l, for example, $0^l = \underbrace{00\cdots0}_{l}$.)

1. Uniform distribution over $\mathcal{K}$.
2. Uniform distribution over $\mathcal{K} \setminus \{0^l\}$, where $\setminus$ means removing one element from the set.
3. $P(K = k) = \begin{cases} 1/2 & \text{if } k = 0^l \\ 1/2 & \text{if } k = 1^l \\ 0 & \text{others} \end{cases}$
4. $P(K = k) = \begin{cases} 1/2^{l-1} & \text{if the number of bits that equal to 1 in } k \text{ is odd.} \\ 0 & \text{others} \end{cases}$
5. None of the above.

Solution

- Exact answer: 1

The OTP's distribution of keys must be uniform; otherwise, certain messages will exhibit higher probabilities when given the ciphertext, thereby violating the principle of perfect secrecy.

For the following five questions starting at Question 3 Let (Enc, Dec) be a semantically secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^l$. Let $H : \{0,1\}^* \to \{0,1\}^l$ be a cryptographically secure hash function. Which of the following encryption algorithms in Question 2 to Question 6 are necessarily semantically secure? Select "True" if it is semantically secure; False otherwise. (Let $x||y$ represent concatenation of x and y) Please provide your explanation.

1. **Question 3** (2 pts). $E(k,m) = Enc(k, m \oplus 1^l)$
2. **Question 4** (2 pts). $E(k,m) = Enc\big(1^l \oplus k, m\big)$
3. **Question 5** (2 pts). $E(k,m) = Enc(k, Enc(k,m))$.
4. **Question 6** (2 pts). $E(k,m) = Enc(k,m)||H(m)$.
5. **Question 7** (2 pts). $E(k,m) = Enc(k,m)||H(Enc(k,m))$, where $H : \{0,1\}^* \to \{0,1\}^l$ is a deterministic cryptographic hash function.

Solution

1. **Question 3** (2 pts). $E(k,m) = Enc(k, m \oplus 1^l)$
   - **Answer**: True
   - **Explanation**: The encryption is semantically secure because it relies on the semantically secure cipher Enc. The XOR operation with 1^l is a deterministic transformation. Specifically, $Pr[C = c|M = m] = Pr[C = c|M = m \oplus 1^l]$ for all $m \in \mathcal{M}, c \in \mathcal{C}$.
2. **Question 4** (2 pts). $E(k,m) = Enc\big(1^l \oplus k, m\big)$
   - **Answer**: True
   - **Explanation**: The encryption is semantically secure. The XOR operation won't change the key distribution
3. **Question 5** (2 pts). $E(k,m) = Enc(k, Enc(k,m))$
   - **Answer**: False
   - **Explanation**: If Enc is OTP, then $E(k,m)$ will always show plaintext
4. **Question 6** (2 pts). $E(k,m) = Enc(k,m)||H(m)$
   - **Answer**: False
   - **Explanation**: The hash of the plaintext m is directly appended to the ciphertext, adversary can choose plaintext with different hash value in bit guessing game.
5. **Question 7** (2 pts). $E(k,m) = Enc(k,m)||H(Enc(k,m))$
   - **Answer**: True
   - **Explanation**: If not, then adversary can compute the appended hash $H(Enc(k,m))$ and win the bit gussing game on Enc with the same advantage, which conflicts the assumption that Enc is semantic secure.

For the following four questions starting at Question 8. Recall the definition of collision resistance for hash functions: It is hard to find two distinct inputs m_1 and m_2 (where $m_1 \neq m_2$) such that $H(m_1) = H(m_2)$. Assume H is collision resistant. Consider the H' hash function in each of the following questions (Question 8 to Question 11), and determine if it is collision-resistant. Select "True" if a hash function is collision-resistant, and "False" otherwise.

1. **Question 8** (2 pts). $H'(m) = m[1]||H(m[2,..,|m|])$, i.e., concatenation of the first bit of m with the hash of the remaining part of m (from the second bit).
2. **Question 9** (2 pts). $H'(m) = H(m[1,..,|m|-1])$, i.e., hash m without its last bit.
3. **Question 10** (2 pts). $H'(m) = H(m||m)$, i.e., hash the concatenation of m and m.
4. **Question 11** (2 pts). $H'(m) = H(m||m \oplus 1^{|m|})$, i.e., hash the concatenation of m and $m \oplus 1^{|m|}$.

Solution

1. **Question 8** (2 pts). $H'(m) = m[1]||H(m[2,..,|m|])$
   - **Answer**: True
   - **Explanation**: Yes, if there exists some adversary A' finding collisions of H' efficiently, which can be reduced to make an adversary A that asks for collisions for H' from A' and drops the first bit.
2. **Question 9** (2 pts). $H'(m) = H(m[1,..,|m|-1])$
   - **Answer**: False
   - **Explanation**: No, for two messages which differ only in the last bit, the hash function results in the same output.
3. **Question 10** (2 pts). $H'(m) = H(m||m)$
   - **Answer**: True
   - **Explanation**: Yes, as any collision in H' will result in a collision in H.
4. **Question 11** (2 pts). $H'(m) = H(m||m \oplus 1^{|m|})$
   - **Answer**: True
   - **Explanation**: Yes, as any collision in H' will result in a collision in H.

Question 12. (3 pts).
Let H_1 and H_2 be two collision resistant hash functions, with the same output size. Which of the following constructions of H' are collision resistant hash functions? Choose all the correct answers. Provide your explanation.

a $H'(m) = H_1(m) \oplus H_2(m)$.

b $H'(m) = H_1(m)||H_2(m)$.

c $H'(m) = H_1(H_2(m))$

d None of the above.

Solution

a $H'(m) = H_1(m) \oplus H_2(m)$

- **Answer**: No
- **Explanation**: H_1 and H_2 could be complements of each other, making it possible to find collisions in H'.

b $H'(m) = H_1(m)||H_2(m)$

- **Answer**: Yes
- **Explanation**: Any collision in H' will result in a collision in either H_1 or H_2, both of which are assumed to be collision-resistant.

c $H'(m) = H_1(H_2(m))$

- **Answer**: Yes
- **Explanation**: Any collision in H' will result in a collision in H_1 or H_2, both of which are assumed to be collision-resistant.

d None of the above

- **Answer**: No
- **Explanation**: Options b and c are collision-resistant.

Question 13. (5 pts).
Is it possible for an encryption scheme to inadvertently reveal information about its key (meaning, you can construct an encryption scheme for which there exists $k \in \mathcal{K}$ such that $P(K = k|C = c) \neq P(K = k)$), while still maintaining perfect secrecy? Please provide an explanation for your answer.

Solution Answer: Yes

Explanation: Consider "double OTP" $Enc(k_1, k_2, m) = k_1||k_1 \oplus k_2 \oplus m$

Question 14. (4 pts).
Recall that in ECB (Electronic Codebook) mode of composing block ciphers, each block of the plaintext is independently encrypted using the symmetric key k. Does a block cipher constructed in ECB mode provide CPA (Chosen Plaintext Adversary) security? Why?

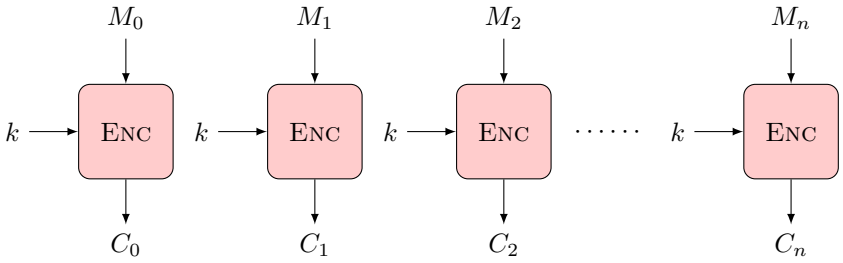

Figure 1: ECB Encryption

Solution Answer: No
Explanation: ECB mode does not provide CPA security because the encryption is deterministic. In other words, a given plaintext block will always result in the same ciphertext block when encrypted with the same key. An adversary can exploit this property to learn information about the plaintext from the ciphertext, thereby violating the CPA security definition.

Question 15. (5 pts).
Authenticated encryption schemes provide both message integrity and confidentiality. We use Enc to encrypt messages and (S, V) for MAC (S is the signing function and V is the corresponding verification function). We also use a cryptographically secure hash function H. The established symmetric keys for encryption and MAC are denoted k_1 and k_2. These keys are unknown to the adversary. We concatenate using $||$.

Suppose we construct the following three protocols for communicating m.

1. Protocol I: $Enc\big(k_1, m\big) \,||\, S\left(k_2, Enc\big(k_1, m\big)\right)$.
2. Protocol II: $Enc(k_1, m) \,||\, S(k_2, m)$.
3. Protocol III: $Enc(k_1, m) \,||\, H(m)$.

Which of the following descriptions about the confidentiality and integrity of the above schemes are true? Choose all correct answers. Explain your answers.

1. Protocol I satisfies CPA security (confidentiality).
2. Protocol II satisfies CPA security (confidentiality).
3. Protocol I satisfies integrity.
4. Protocol III satisfies integrity.
5. None of the above.

Solution 1,3

- Protocol II doesn't satisfies CPA security because MAC does not ensure confidentialiy
- Protocol III doesn't satisfy integrity because everyone can compute the hash.

Question 16. (5 pts).

We know that the "textbook" RSA is not secure. But, Alice and Bob insist to use it in their message exchange protocol. Their public key and secret key pairs are $((e_A, n), d_A)$ and $((e_B, n), d_B)$ respectively. Alice encrypts a message m using Bob's public key to get $c = m^{e_B} \mod n$, which only Bob can decrypt, and sends it to Bob. We want to show them what can go wrong.

A man-in-the-middle attacker modifies the ciphertext c and replaces it with c' (i.e., Bob receives c' and not c). What should be the value of c' such that when Bob decrypts it, it gets decrypted to $2m$. Assume $n = 21$, $e = 3$ and $c = 2$. Please also provide the details of your solution.

Solution We are given that

$$c = m^e \mod n.$$

To find $c' = (2m)^e \mod n$, we can perform the following mathematical manipulations:

$$\begin{aligned} c' &= (2m)^e \mod n \\ &= 2^e \times (m^e) \mod n \\ &= 2^e \times c \mod n \end{aligned}$$

Since both e and c are public, we can easily compute c':

$$\begin{aligned} c' &= 2^3 \times 2 \mod 21 \\ &= 16 \mod 21 \\ &= 16 \end{aligned}$$

Question 17. (4 pts)
Recall the Diffie-Hellman Protocol.

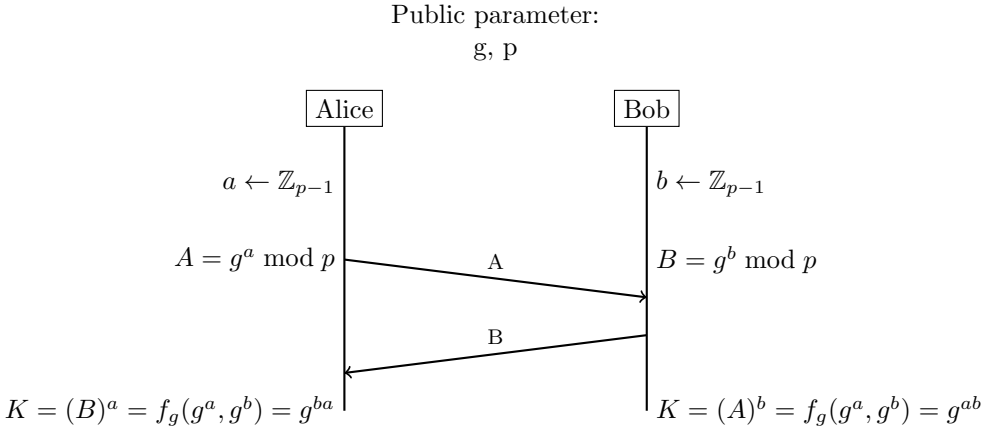

Figure 2: Diffie Hellman Key Exachange

Consider the following alternative constructions of the key. Is it secure to use the following function f'_g as the key instead of f_g? Choose all that you think it's secure.

1. $f'_g(g^a, g^b) = g^{(a+b)}$
2. $f'_g(g^a, g^b) = g^{ab+1}$
3. $f'_g(g^a, g^b) = g^{(2a+b)}$

Explain your response.

Solution

1. $f'_g(g^a, g^b) = g^{(a+b)}$
   - **Answer**: No
   - **Explanation**: This is not secure because $g^{(a+b)}$ can be easily computed by an eavesdropper who knows g^a and g^b. The function f'_g does not maintain the secrecy of the shared key.
2. $f'_g(g^a, g^b) = g^{ab+1}$
   - **Answer**: Yes
   - **Explanation**: This is secure because an algorithm for $f'_g(g^a, g^b)$ can easily be converted into an algorithm for calculating $f_g(g^a, g^b) = g^{ab}$. The function f'_g maintains the secrecy of the shared key.
3. $f'_g(g^a, g^b) = g^{(2a+b)}$
   - **Answer**: No
   - **Explanation**: This is not secure because $g^{(2a+b)}$ can be computed by an eavesdropper who knows g^a and g^b. The function f'_g does not maintain the secrecy of the shared key.

For the next two questions starting from Question 18 Recall that in Randomized CBC mode, the first block of the plaintext is encrypted using a random IV (which is communicated in the beginning of the protocol) and the secret symmetric key. Every subsequent plaintext block is encrypted using the ciphertext of the previous block and the symmetric key.

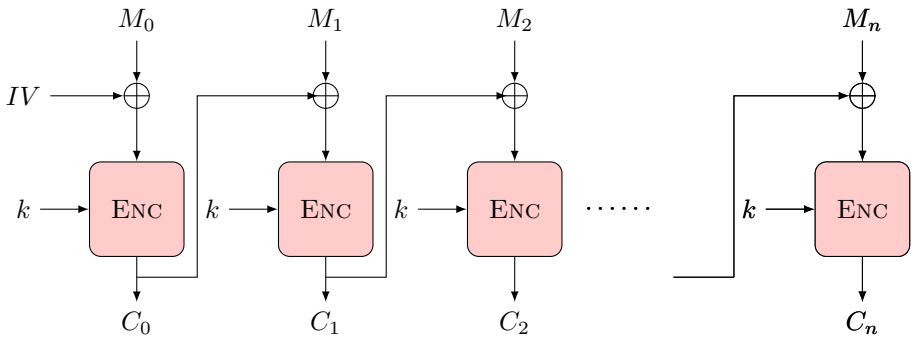

Figure 3: CBC Encryption

You need to show that randomized CBC encryption using AES does not preserve message integrity. Suppose adversary intercepts the IV

`323565478b52038c659360ecd8638532`

and intercepts also the first block of ciphertext (i.e. C_0):

`b365828d548b3f742504e7203123218a`

You know that the ciphertext is an encryption of the plaintext "To:bob@gmail.com", where the plaintext is encoded as ASCII bytes. The first 16-byte block is the IV and the second 16-byte block carries the message. Modify the ciphertext above so that it decrypts to the message "To:mel@gmail.com". Your answer should be the two block modified ciphertext. You may refer to the attached ASCII TABLE and HEX XOR TABLE.

Question 18. (3 pts). What is the modified IV?

Question 19. (3 pts) What is the modified ciphertext?

Solution

- "32356548815c038c659360ecd8638532"
- "b365828d548b3f742504e7203123218a"

Consider how the first (and only) ciphertext block c is decrypted. The decryption can be represented as:

$$m = \text{Dec}(k, c) \oplus \text{IV}$$

Let a be a value such that when XORed with the initial value (IV), it mutates the plaintext m to $m \oplus a$. The decryption with this mutated initial value can be represented as:

$$m \oplus a = \text{Dec}(k, c) \oplus (\text{IV} \oplus a)$$

We want to find a such that the mutated plaintext gives us the desired result:

$$\text{"To:bob@gmail.com"} \oplus a = \text{"To:mel@gmail.com"}$$

Solving for a, we get:

$$a = \text{"To:mel@gmail.com"} \oplus \text{"To:bob@gmail.com"}$$

Then, the modified IV' is given by:

$$\text{IV'} = \text{IV} \oplus a = \text{IV} \oplus (\text{"To:mel@gmail.com"} \oplus \text{"To:bob@gmail.com"})$$

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Hex xor Table

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	F
0	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	1	0	3	2	5	4	7	6	9	8	b	a	d	c	f	e
2	2	3	0	1	6	7	4	5	a	b	8	9	e	f	c	d
3	3	2	1	0	7	6	5	4	b	a	9	8	f	e	d	c
4	4	5	6	7	0	1	2	3	c	d	e	f	8	9	a	b
5	5	4	7	6	1	0	3	2	d	c	f	e	9	8	b	a
6	6	7	4	5	2	3	0	1	e	f	c	d	a	b	8	9
7	7	6	5	4	3	2	1	0	f	e	d	c	b	a	9	8
8	8	9	a	b	c	d	e	f	0	1	2	3	4	5	6	7
9	9	8	b	a	d	c	f	e	1	0	3	2	5	4	7	6
a	a	b	8	9	e	f	c	d	2	3	0	1	6	7	4	5
b	b	a	9	8	f	e	d	c	3	2	1	0	7	6	5	4
c	c	d	e	f	8	9	a	b	4	5	6	7	0	1	2	3
d	d	c	f	e	9	8	b	a	5	4	7	6	1	0	3	2
e	e	f	c	d	a	b	8	9	6	7	4	5	2	3	0	1
F	f	e	d	c	b	a	9	8	7	6	5	4	3	2	1	0

For the next three questions starting from Question 20. Assume a TLS connection has been established between an honest client and server. Assume that the keys are NOT compromised. Does TLS protect against the following attacks? Answer "True" if TLS is secure against the attack, and "False" if TLS does not protect against the attack.

Question 20. (1 pts). An attacker modifying the ciphertext sent from the client to the server such that it decrypts to the message of the attacker's choice.

Question 21. (1 pts). An attacker impersonating the server.

Question 22. (1 pts). An attacker identifying the web page that the user is connecting to, among all the web pages hosted at the server.

Solution

1. **Question 1** (1 pts). An attacker modifying the ciphertext sent from the client to the server such that it decrypts to the message of the attacker's choice.
   - **Answer**: True
   - **Explanation**: TLS uses authenticated encryption, which ensures both confidentiality and integrity of the messages. Therefore, any modification to the ciphertext would be detected.
2. **Question 2** (1 pts). An attacker impersonating the server.
   - **Answer**: True
   - **Explanation**: TLS uses public key infrastructure and certificates to authenticate the server, making it difficult for an attacker to impersonate the server without the private key.
3. **Question 3** (1 pts). An attacker identifying the web page that the user is connecting to, among all the web pages hosted at the server.
   - **Answer**: False
   - **Explanation**: While TLS encrypts the content of the communication, metadata like the IP address and possibly the specific page being accessed (through SNI, Server Name Indication) may still be visible to an eavesdropper.