March 19th, 2018

German University in Cairo
Media Engineering and Technology
Lecturer: Amr El Mougy
TA: Alaa Gohar

Computer and Network Security

Spring term 2018
Midterm Exam

Bar Code

Instructions: Read carefully before proceeding.

1) Duration of the exam: 2 hours (120 minutes).
2) (Non-programmable) Calculators are allowed.
3) No books or other aids are permitted for this test.
4) This exam booklet contains 9 pages, including this one. **Note that if one or more pages are missing, you will lose their points. Thus, you must check that your exam booklet is complete.**
5) Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem or on the extra sheets and make an arrow indicating that.
6) When you are told that time is up, stop working on the test.
7) Include any assumptions that you need to make.
8) Follow the instructions of your proctors under all circumstances.

Good Luck!

Don’t write anything below ;-)

	1	2	3	4	5	Σ
Marks	10	15	20	20	20	85
Final Marks						

Question 1:

Specify if the following statements are True (T) or False (F). If you need to justify your answer, please do so in the space provided.

1) Encryption using AES guarantees message authentication.	F
2) Authenticating the public key in the Diffie-Hellman exchange protects against replay attacks.	F
3) The Initial Value (IV) in the Cipher Block Chaining (CBC) mode has the same confidentiality requirements as the encryption key.	F
4) In end-to-end encryption (such as encryption of application layer data), only the original source and the final destination need to have the key.	T
5) The weak collision resistance property of hash functions specifies that it should be computationally infeasible to find any two values x and y such as $H(x) = H(y)$.	F
6) The birthday attack on hash functions has complexity $2^{m/2}$, where m is the size of the produced hash in bits.	T
7) The HMAC function does not require a key.	F
8) An attack on a MAC requires the observation of several messages, and their MACs, generated using the same key.	T
9) In Diffie-Hellman, if the generator "a" is not a primitive root mod q, where q is the chosen prime number, the algorithm will not result in the two parties deriving the same key (*i.e.* the algorithm will not work).	T
10) One way to generate a digital signature is to encrypt the hash of a message with the public key of the receiver.	F

Extra space for justification (only if needed):

Question 2:

a) The Vigenere autokey cipher is a modification over the traditional Vigenere cipher, where the key that is used for encryption is generated from a passphrase plus the plaintext itself. For example, to encrypt the phrase "*Ilovesecurity*" using the passphrase "*frog*", the encryption key becomes "*frogIlovesecu"*. What does this modification intend to solve? Is the Vigenere autokey more secure than traditional Vigenere?

b) A two-stage encryption algorithm is built using a Vigenere autokey cipher followed by a transposition cipher. The passphrase for the Vigenere autokey cipher is "goal" and the key for the transposition cipher is 3 5 4 1 2. Decrypt the following ciphertext to obtain the plaintext.

LFTWUXNQVKSOUWASRHTBCZZJJ

Answer 2:

a) There are no more key repetitions. Thus, the Kasiski method will not work. It is therefore more secure.

b)

3	5	4	1	2
S	C	S	L	X
O	Z	R	F	N
U	Z	H	T	Q
W	J	T	W	V
A	J	B	U	K

Decryption of transposition is SCSLXOZRFNUZHTQWJTWVAIJBUK

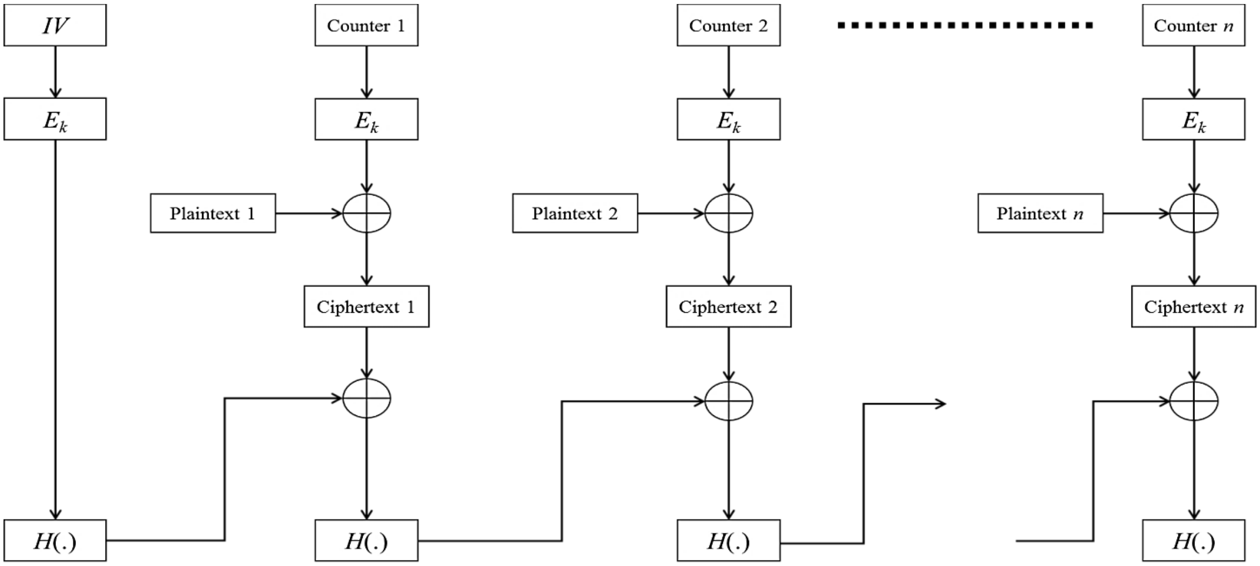
Decrypt the first 4 letters SCSL using the passphrase "goal" gives MOSA. Thus, we decrypt the next 4 letters XOZR using MOSA to get LAHR

We continue to get the phrase MOSALAHRUNNINGDOWNTHEWING

Or *Mo Salah Running Down The Wing!!*

Question 3:

The figure below shows a mode of encryption known as Galois Counter Mode (GCM). In the figure, *IV* is an initial value that is used only in the first stage of encryption and changed for every group of encrypted blocks. For every block of plaintext, a counter is incremented and encrypted (E_k) using key *k*. In addition, *H*(.) is the hash of the value (.), and ⊕ denotes the XOR operation.



a) Which security objectives does this mode achieve (confidentiality, integrity, authentication, non-repudiation)?

b) What should be the security requirements of the IV?

c) Draw a figure for the decryption algorithm.

Answer:

a) The CTR mode achieves confidentiality while the chained hash provides authentication and integrity.

b) Same as CBC. Not predictable at encryption time.

c) Same as encryption but replace ciphertext with plaintext. The output of the hash is chained and compared in the last step.

Question 4:

One solution to the Man-In-The-Middle problem in Diffie-Hellman is to digitally-sign the public keys. Thus, we consider a system where Alice and Bob use a combination of RSA and Diffie-Hellman for authenticated key exchange. For Diffie-Hellman, Alice and Bob agree on a prime number 199 and its primitive root 15. Alice chooses her Diffie-Hellman private key 6, while Bob chooses 10. On the other hand, for RSA, Alice has public key {5, 493}, while Bob has public key {25, 551}.

Accordingly, in this system, when Alice and Bob would like to exchange a key using Diffie-Hellman, they send two items, the plain Diffie-Hellman public key and the digitally signed Diffie-Hellman public key using RSA. This algorithm is summarized in the table below.

Alice	*Bob*
1. Generate the Diffie-Hellman private key (x_A) and calculate the public key (y_A). 2. Digitally sign the Diffie-Hellman public key (y_A) using RSA. Let the result be DS(y_A). 3. Send to Bob {y_A || DS(y_A)}	1. Generate the Diffie-Hellman private key (x_B) and calculate the public key (y_B). 2. Digitally sign the Diffie-Hellman public key (y_B) using RSA. Let the result be DS(y_B). 3. Send to Alice {y_B || DS(y_B)}

a) If bob receives from Alice the combination {64, 13}, is the Diffie-Hellman public key verified in this case?

b) If yes, what is the corresponding exchanged key (the result of the Diffie-Hellman exchange)? If no, what should be the correct combination sent and what is the corresponding exchanged key?

Answer:

a) Bob has to verify the signature. Thus, Bob has to decrypt it using Alice’s public key. The decryption is 13^5 mod 493 = 64. Thus, the signature is verified.

b) Now Bob can calculate the exchanged key using 64^{10} mod 199 = {(64^4 mod 199) (64^4 mod 199) (64^2 mod 199)} mod 199 = {(123)(123)(116)} mod 199 = 182

Question 5:

a) A particular MAC uses a key of size 256 bits and the tag produced has size 128 bits. How many (message, MAC) pairs, generated using the same key, must the attacker observe in order to be able to brute force the key?

b) The following statements show different uses of hash functions and MACs. All the shown operations occur at the sender side. Draw a figure and specify a statement for the operations at the receiver side. In addition, for each statement specify which of the following properties are achieved: **confidentiality, integrity, non-repudiation.**

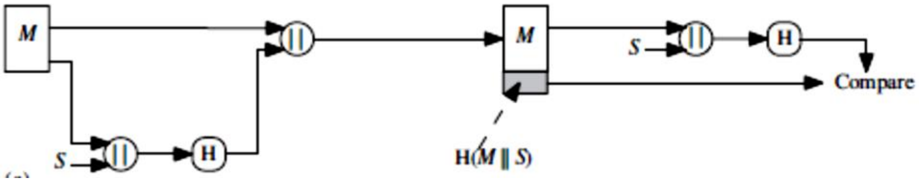
- $M \parallel H(k \parallel M)$
- $M \parallel E(k, H(M))$
- $M \parallel H(M)$
- $E(k, (M \parallel H(M)))$
- $E(k_1, M)||E(k_2, H(M))$

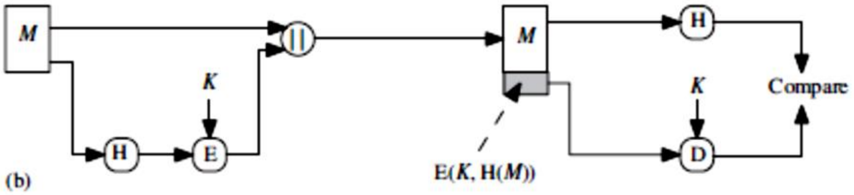
Note that *M* is the message, *H*(.) is the hash of (.), *E*(*x*,.) is symmetric encryption of (.) with key *x*, and || denotes concatenation.

Answer:

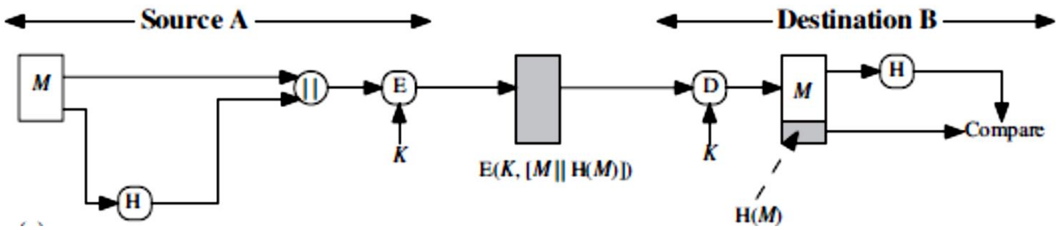
a) First round produces 256 – 128 = 2^{128} possible keys. The second round produces the right key. Thus only two pairs are needed.

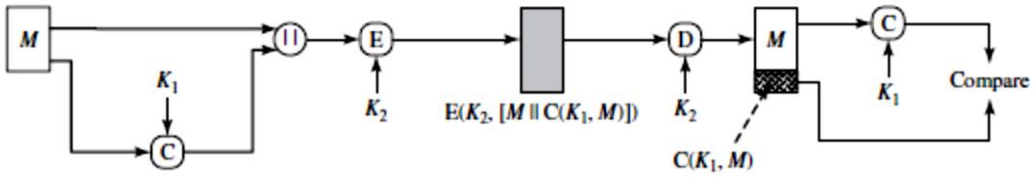
b) Integrity, Integrity, none, confidentiality and integrity, confidentiality and integrity





(b)


Source A
Destination B
M
||
E
K
H
E(K, [M || H(M)])
D
K
M
H
Compare
H(M)


M
K1
C
||
E
K2
E(K2, [M || C(K1, M)])
D
K2
M
C
K1
Compare
C(K1, M)