BBM463: Midterm Exam -25/11/2020

Toplam puan 66/100

E-posta adresi *

b21827852@cs.hacettepe.edu.tr

0 üzerinden 0 puan

Name *

İbrahim Burak Tanrıkulu

Student ID *

21827852

Copying answers from Internet sources or communicating with other students during the exam will be considered as cheating. You must prepare your answers with your own knowledge and not use any external help. However you can use your notes and class slides during the exam. Do you understand and accept this policy? *

- (●) Yes

Questions 100 üzerinden 66 puan

Instructions

- In some questions, answers are longer than one line. When entering multiline answers, you can use Shift+Enter to continue on the next line.
- To show power of a number you can use ^ symbol, such as 2^3 for 2^3.
- To show subscript you can use _ symbol, such as A_X for A_X.
- Assume that an alphabet with 26 letters is used for basic ciphers.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
π=	B	A	D	C	Z	H	W	Y	G	O	Q	X	S	V	T	R	N	M	L	K	J	I	P	F	E	U

In an encryption operation using a mono-alphabetical substitution cipher, the above conversion function is used. With this information, please answer the **following four questions**. (You can leave computational answers in the form of products.)

✓ Find the ciphertext of “AESISMORESECURETHANDES” using the above function : 3/3

BZL GL STMZ LZDJMZ KYBV CZL ✗

Doğru cevap

BZLGLSTMZLZDJMZKYBVCZL

✓ Find the plaintext of “ZVGWSBGLBPZLTSZ”, which is encrypted with the above function : 3/3

ENIGMAISAWESOME ✓

✓ Find the total number of key combinations if the above algorithm is used with a Vigenere Cipher with a key length of 4. (That means we apply the above mono-alphabetical substitution cipher first and then Vigenere Cipher to encrypt our plaintext) : 4/4

29!*29^4 ✗

Doğru cevaplar

26!. 26^4

26! x 26^4

✓ Find the total number of key combinations if each letter in the conversion function is changed with one of the numbers between 1 and 99: 4/4

99!/73! ✗

Doğru cevap

99.98.97....74

✗ On Enigma machine with 5 rotors, how many different key combinations can be generated? 1/2

26^5 ✗

Doğru cevaplar

26^5 x 5!

26^5 . 5!

5! x 26^5

5! . 26^5

✗ On Enigma machine with 5 rotors, assume that you know the first rotor and its start position. How many key combinations can be generated with the other 4 rotors? 1/3

26^3 ✗

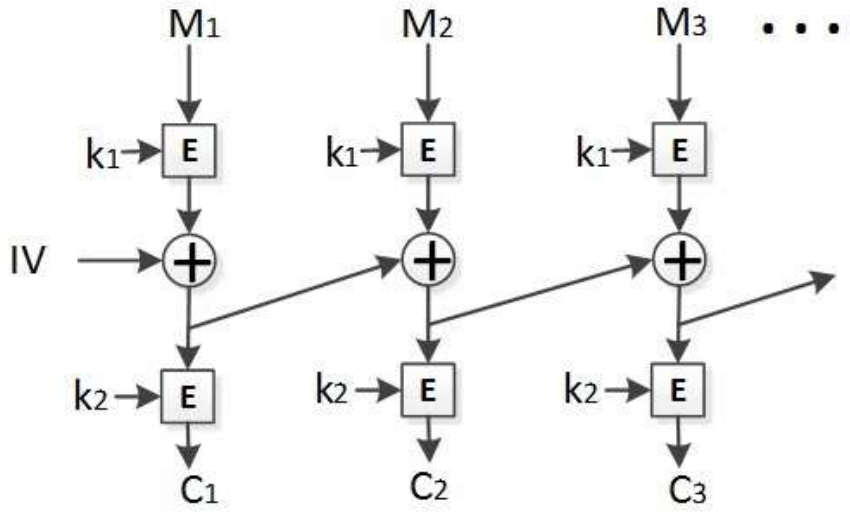
Doğru cevaplar

26^4 x 4!

26^4 . 4!

4! . 26^4

4! x 26^4



The above figure shows an encryption mode. k_1 and k_2 are key values used by the encryption algorithm (E). IV is the initialization vector. (+) is the exclusive-or operation. While $M_1,M_2,M_3,...$ are plaintext blocks, $C_1,C_2,C_3,...$ are ciphertext blocks. Answer the **following three questions** according to this diagram. (Use D symbol for the decryption operation).

✗ Define the above encryption mode as a mathematical expression. 4/5

X_0 = IV, X_i = E_k1[M_(i-1)] (+) X_(i-1), C_i = E_k2[X_i (+) E_k1[M_i]]

✗ Define the decryption operation as a mathematical expression. (Hint: Drawing the decryption operation like the above figure might help) 2/5

X_0 = IV, X_i = D_k2[C_(i-1)] (+) X_(i-1), C_i = D_k1[X_i (+) D_k2[M_i]]

✗ Assume that one bit of C_2 is corrupted while transmitting it over Internet. Which plaintext messages are lost in this case? Explain your answer. 2/4

Corruption of C_2 causes to generate wrong X_i vectors for next "D_k2"s. So just M1 will be right but others will be corrupted.

✓ Double DES is vulnerable to meet-in-the-middle attacks, but Triple DES is not. Why is Triple DES more secure against meet-in-the-middle attacks? Explain your answer. 8/8

In Double DES:
E[E[P]] = C ---> E[P] = D[C] ---> 2^56 + 2^56 = 2^57 combinations.
But in Triple DES:
E[E[E[P]]] = C ---> E[E[P]] = D[C] or E[P] = D[D[C]] .
Thus Triple DES is more secure; 2^112 + 2^56 combinations

✗ Hill cipher is not secure since it contains linear transformations. Which internal components of DES algorithm help to satisfy nonlinearity requirement for better security? Explain how these components enable nonlinearity of DES algorithm. 4/8

Non-linear S-Boxes enables nonlinearity. Output is smaller then input.

OFB	CTR
$K_i = E_K(K_{i-1}), \quad K_0 = IV$	$K_i = E_K(counter+i)$
$C_i = P_i \oplus K_i$ (encryption) $P_i = C_i \oplus K_i$ (decryption)	$C_i = P_i \oplus K_i$ (encryption) $P_i = C_i \oplus K_i$ (decryption)

The above table shows the generation of the key sequence in the OFB and CTR encryption modes using a symmetric encryption algorithm (E) and K secret key. Encryption and decryption operations are performed with simple XOR operations. **For each encryption mode, describe separately** how the key sequence (K_i) can be generated using **a hash function (H)** instead of an encryption algorithm. Use mathematical expressions as shown above.

✗ OFB: 3/5

K_0 = IV , K_i = H[K_(i-1)]

✗ CTR: 3/5

K_i = H[counter+i]

✓ Assume that the cars in the department's parking area can be in 10 different colors and all colors are in uniform distribution. What is the probability of that 4 cars in the parking area have different colors? Show your calculations. You can give an approximate value. 5/5

Birthday paradox problem.
First car parked and we know the color now.
Second car's color's probability of different color is 9/10.
Third car's color's probability of different color is 8/10.
Forth car's color's probability of different color is 7/10.
So our calculation is 9/10 * 8/10 * 7/10 = 504/1000

✗ Assume that Alice and Bob share p and q values, which are large prime numbers. They use these numbers to calculate n=p.q value for the RSA algorithm. Then, Alice chooses (e_A, d_A) parameters as in the RSA algorithm and Alice announces (e_A, n) values as her public key. Similarly, Bob chooses (e_B, d_B) parameters and announces (e_B, n) values as his public key. Is it secure to use the same n value for Alice? Can Bob do an attack on Alice's RSA keys? Explain your answer 1/8

It is still secure. Because; lets say we have n, e. We must find d to decrypt.
d = e^-1 mod phi(n).
There are a lot of d values in there. We must try a lot of combinations that
ed = 1 mod phi(n).

✗ 7/10

You are asked to configure a company's firewall according to the following rules:
1) All packets from the local network to the external network will be allowed.
2) All HTTP packets from the external network to the "WEBGW" server on the local network will be allowed.
3) All SMTP packets from the external network to the "MAILGW" server on the local network will be allowed.
4) All HTTP, SMTP, and DNS packages from "BLACKHAT" site will be rejected.
5) All ACK packets of a continuing communication from the external network to the local network will be allowed.
6) All other packages will be denied.
According to these rules, fill in the following firewall setting table. Actions can be either ALLOW or DENY. Denote the local network as "LOCAL" and the external network as "EXTERNAL". (6 pts)

Note: When a packet is evaluated on a firewall, the rules are examined in increasing order (starting from rule 1). The operation stops when a matching rule is found. Fill the table according to this execution principle! You can add rows to the table if necessary.

Rule	Action	Source	Port	Destination	Port	Flags
1						
2						
3						
...						

1 ALLOW "LOCAL" * "EXTERNAL" * *
2 ALLOW "EXTERNAL" http "WEBGW" * *
3 ALLOW "EXTERNAL" smtp "MAILHW" * *
4 DENY "BLACKHAT" HTTP * * *
5 DENY "BLACKHAT" SMTP * * *
6 DENY "BLACKHAT" DNS * * *
7 ALLOW "EXTERNAL" * "LOCAL" * ACK
8 DENY * * * * *

1. Firewall 2. Internal Firewall 3. Site-to-Site VPN 4. Remote Access VPN	5. Extranet VPN 6. Internal VPN 7. SIEM 8. IDS/IPS

Please match each of the below tasks with **the most suitable** network security tool. (You don't have to match all of these tools to the tasks, some tools may not be used.)

✓ Filtering packages that are sent to a part of the local network from other parts of the local network. 1/1

1. Firewall
2. Internal Firewall ✓
3. Site-to-Site VPN
4. Remote Access VPN
5. Extranet VPN
6. Internal VPN
7. SIEM
8. IDS/IPS

✓ Analyzing all network traffic and detecting suspicious packets. 1/1

1. Firewall
2. Internal Firewall
3. Site-to-Site VPN
4. Remote Access VPN
5. Extranet VPN
6. Internal VPN
7. SIEM
8. IDS/IPS ✓

✗ Detecting a malicious login operation in the local network, which violates the company's security policies. 0/1

1. Firewall
2. Internal Firewall
3. Site-to-Site VPN
4. Remote Access VPN
5. Extranet VPN
6. Internal VPN ✗
7. SIEM
8. IDS/IPS

Doğru cevap

SIEM

✓ Filtering packages that are sent to the local network from the external network. 1/1

1. Firewall ✓
2. Internal Firewall
3. Site-to-Site VPN
4. Remote Access VPN
5. Extranet VPN
6. Internal VPN
7. SIEM
8. IDS/IPS

✗ Securing the communication between multiple remote offices of the company. 0/1

1. Firewall
2. Internal Firewall
3. Site-to-Site VPN
4. Remote Access VPN
5. Extranet VPN ✗
6. Internal VPN
7. SIEM
8. IDS/IPS

Doğru cevap

Site-to-Site VPN

✓ Enabling a secure connection to an internal server for an employee, who is working outside of the local network. 1/1

1. Firewall
2. Internal Firewall
3. Site-to-Site VPN
4. Remote Access VPN ✓
5. Extranet VPN
6. Internal VPN
7. SIEM
8. IDS/IPS

✓ Analyzing all network logs and detecting suspicious activity. 1/1

1. Firewall
2. Internal Firewall
3. Site-to-Site VPN
4. Remote Access VPN
5. Extranet VPN
6. Internal VPN
7. SIEM ✓
8. IDS/IPS

✗ Enabling a secure connection between different parts (or departments) of the local network. 0/1

1. Firewall
2. Internal Firewall
3. Site-to-Site VPN ✗
4. Remote Access VPN
5. Extranet VPN
6. Internal VPN
7. SIEM
8. IDS/IPS

Doğru cevap

Internal VPN

Bob sends Alice his public key certificate signed by Hacettepe University. Alice first verifies the validity of the certificate. Then Bob signs a message with his private key and sends it to Alice. Alice checks the validity of the signed message. Alice does not trust Hacettepe University as a certification authority, but trusts to TÜBİTAK as a certification authority. According to this information, fill in the following statements appropriately.

To verify Bob's certificate, Alice needs a certificate for .....1..... that is signed by .....2..... By using the public key of .....3..... in this certificate, Alice can verify Bob's certificate. After this verification, Alice can check the validity of the signature in the signed message by using .....4.....'s public key obtained from .....5.....'s certificate."

	Alice	Bob	Hacettepe Un.	TÜBİTAK	Puan	
1	○	○	◉	○	2/2	✓
2	○	○	○	◉	2/2	✓
3	○	◉	○	○	0/2	✗
4	○	◉	○	○	2/2	✓
5	○	○	◉	○	0/2	✗

Doğru cevaplar

	Alice	Bob	Hacettepe Un.	TÜBİTAK
3	○	○	◉	○
5	○	◉	○	○