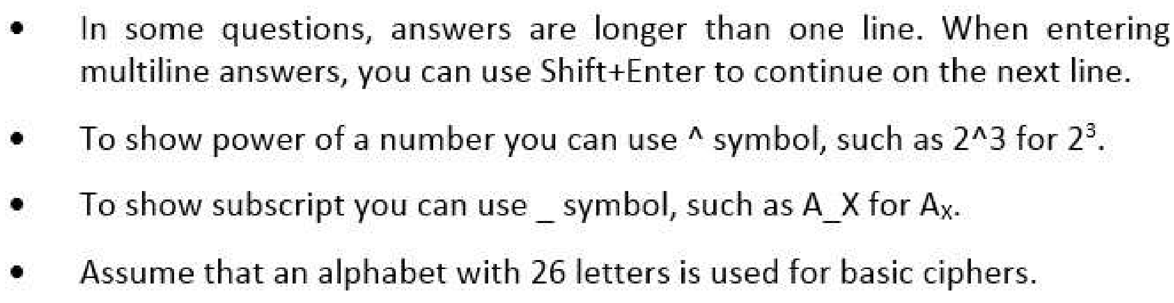
# BBM463: Final Exam -14/01/2021

Dosya yükleyip bu formu gönderdiğinizde Google hesabınızla ilişkili ad ve fotoğraf kaydedilecek. **iburaktk482@gmail.com** size ait değil mi? Hesabı değiştirin

Questions

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.

Q1. In DES's round function, eight S-boxes take 48 bit input and produce a 32 bit output in total. If you know the 32 bit output, what are total number of possible inputs?

4 puan

Yanıtınız

Q2. A hash function produces 256 bits message digests. In order to consider this hash function as collision resistant, at least how many hash operations should be performed by an attacker to find a collision?

2 puan

Yanıtınız

Q3. Assume that the encryption function is C_i=E_k(M_i) ⊕ E_k(C_{i-1}) in an encryption mode (M_i: ith plaintext block, C_i: ith ciphertext block, E_k: Encryption with k key, ⊕: Exclusive OR operation). Define the decryption function (D_k).

5 puan

Yanıtınız

Q4. In the current digital certificate infrastructure, why oligarchy model is preferred ? (or in other words, why other models are not preferred?)

7 puan

Yanıtınız

Q5. Why do we need both AH and ESP services in IPSEC protocol? Isn't ESP enough for all secure communication needs?

7 puan

Yanıtınız

Q6. Even though IPSEC provides more security services than SSL, why do we still use SSL?

7 puan

Yanıtınız

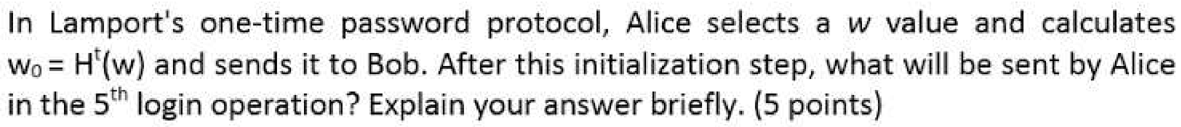
Q7. How did the Slammer worm infect the vulnerable population in a very short time? Why is this worm so fast?

6 puan

Yanıtınız

Q8.

5 puan

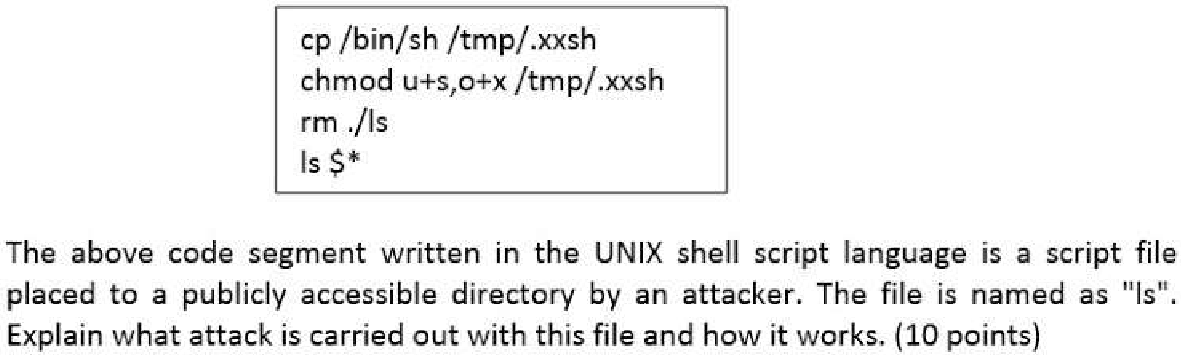


In Lamport's one-time password protocol, Alice selects a *w* value and calculates $w_0 = H^t(w)$ and sends it to Bob. After this initialization step, what will be sent by Alice in the 5th login operation? Explain your answer briefly. (5 points)

Yanıtınız

Q9.

10 puan



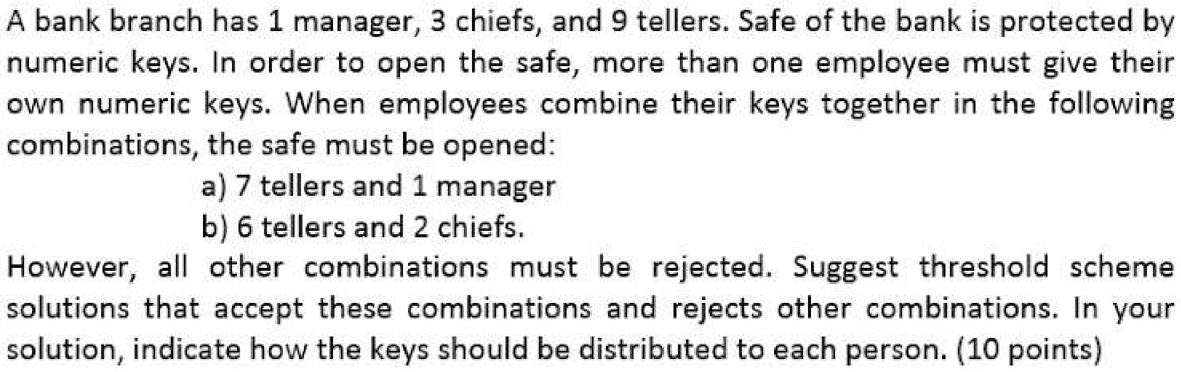
```
cp /bin/sh /tmp/.xxsh
chmod u+s,o+x /tmp/.xxsh
rm ./ls
ls $*
```

The above code segment written in the UNIX shell script language is a script file placed to a publicly accessible directory by an attacker. The file is named as "ls". Explain what attack is carried out with this file and how it works. (10 points)

Yanıtınız

Q10.

10 puan



A bank branch has 1 manager, 3 chiefs, and 9 tellers. Safe of the bank is protected by numeric keys. In order to open the safe, more than one employee must give their own numeric keys. When employees combine their keys together in the following combinations, the safe must be opened:

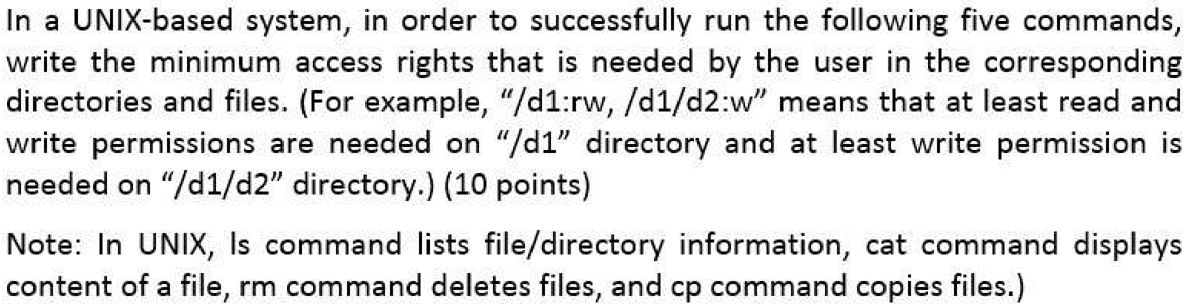
a) 7 tellers and 1 manager

b) 6 tellers and 2 chiefs.

However, all other combinations must be rejected. Suggest threshold scheme solutions that accept these combinations and rejects other combinations. In your solution, indicate how the keys should be distributed to each person. (10 points)

Yanıtınız

Q11.



In a UNIX-based system, in order to successfully run the following five commands, write the minimum access rights that is needed by the user in the corresponding directories and files. (For example, "/d1:rw, /d1/d2:w" means that at least read and write permissions are needed on "/d1" directory and at least write permission is needed on "/d1/d2" directory.) (10 points)

Note: In UNIX, ls command lists file/directory information, cat command displays content of a file, rm command deletes files, and cp command copies files.)

Q11.a) "ls –l /d1/d2/f1" command: 2 puan

Yanıtınız

Q11.b) "cat /d1/d3/f2" command: 2 puan

Yanıtınız

Q11.c) "rm /d1/d4/f3" command: 2 puan

Yanıtınız

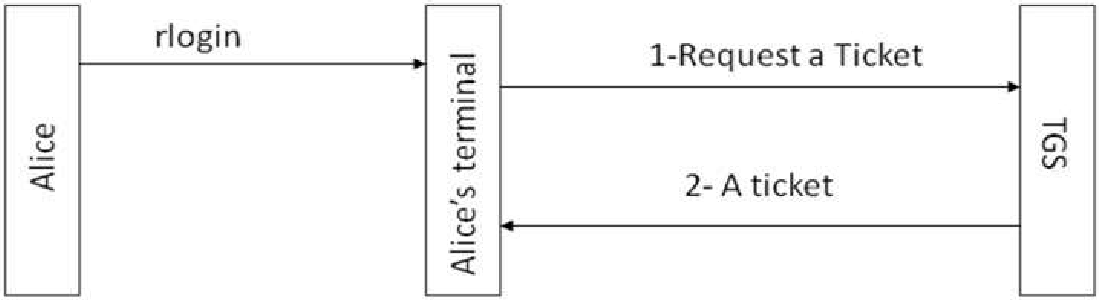
Q11.d) "cp /d1/d2/f4 /d1/f5" command: 2 puan

Yanıtınız

Q11.e) To successfully execute the command "/d1/d2/sc1", where sc1 is a shell script file: 2 puan

Yanıtınız

Q12.



1- Alice → TGS: $ID_B \;||\; Ticket_{tgs} \;||\; Authenticator_A$

2- TGS → Alice: $E_{K_{A,tgs}}[\, K_{AB} \;||\; ID_B \;||\; TS_4 \;||\; Ticket_B \,]$

$Authenticator_A = E_{K_{A,\,tgs}}[\, ID_A \;||\; AD_A \;||\; TS_3 ]$

$Ticket_{tgs} = E_{K_{tgs}}[K_{A,tgs} \;||\; ID_A \;||\; AD_A \;||\; ID_{tgs} \;||\; TS_2 \;||\; Lifetime_2]$

$Ticket_B = E_{K_B}[\, K_{AB} \;||\; ID_A \;||\; AD_A \;||\; ID_B \;||\; TS_4 \;||\; Lifetime_4 \,]$

$ID_A$ ,$ID_B$ : Alice ve Bob sunucusunun kimliği, $AD_A$ : Alice'in adresi

$K_B$ : TGS ve Bob sunucusu arasındaki anahtar

$K_{A,tgs}$ : Alice ve TGS sunucusu arasındaki anahtar

$K_{AB}$ : Alice ve Bob sunucusu arasındaki anahtar

The drawing above shows one phase of Kerberos protocol. Answer the following four questions by considering this drawing (12 points)

Q12.a) What is the purpose of above communication? When this communication happens?

3 puan

Yanıtınız

Q12.b) What is the purpose of Authenticator_A part ? What does TGS do with this part?

3 puan

Yanıtınız

Q12.c) What is the purpose of using ID_A , AD_A in tickets? Why do we need both fields ?

3 puan

Yanıtınız

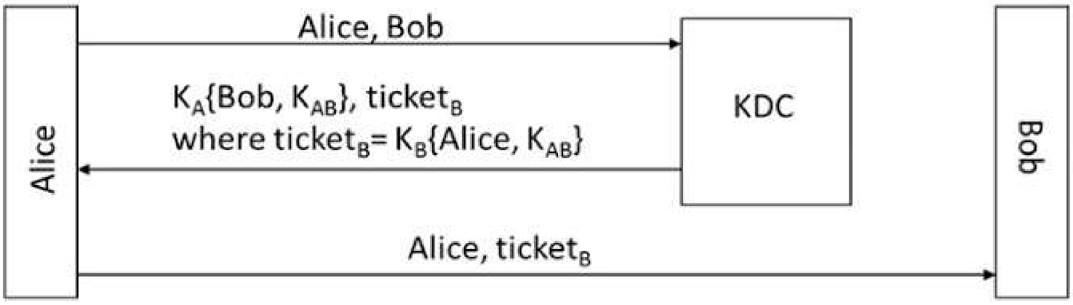
Q12.d) Who does create K_{A,tgs} ? What is the purpose of K_{A,tgs} in Ticket_tgs ?

3 puan

Yanıtınız

Q13.

15 puan


Alice
Alice, Bob
KDC
$K_A\{Bob, K_{AB}\}$, $ticket_B$
where $ticket_B$= $K_B\{Alice, K_{AB}\}$
Alice, $ticket_B$
Bob

In the above authentication protocol, Alice makes a request from the key distribution center (KDC), receives a ticket from KDC, and sends the ticket to Bob to start a session. $K_A$ represents the secret key shared between KDC and Alice. $K_B$ represents the secret key shared between KDC and Bob. The $K_{AB}$ secret key is randomly generated by the KDC to be shared between Alice and Bob. Assume that there is no time synchronization between Alice, KDC and Bob. According to this information, make the following changes to the protocol.

I) One problem with this protocol is that the ticket can be used repeatedly since its lifetime is infinite. Add extensions to the protocol to limit the lifetime of the ticket.

II) Add extensions to the protocol to authenticate Alice (ensure that Alice is using this ticket, not somebody else) before starting session with Bob.

III) Add extensions to the protocol to satisfy perfect forward secrecy of the communication between Alice and Bob (after authentication).

**Explain your answer with a drawing like above. If you define new abbreviations, do not forget to describe them.** (15 points)

Dosya ekle

Geri Gönder