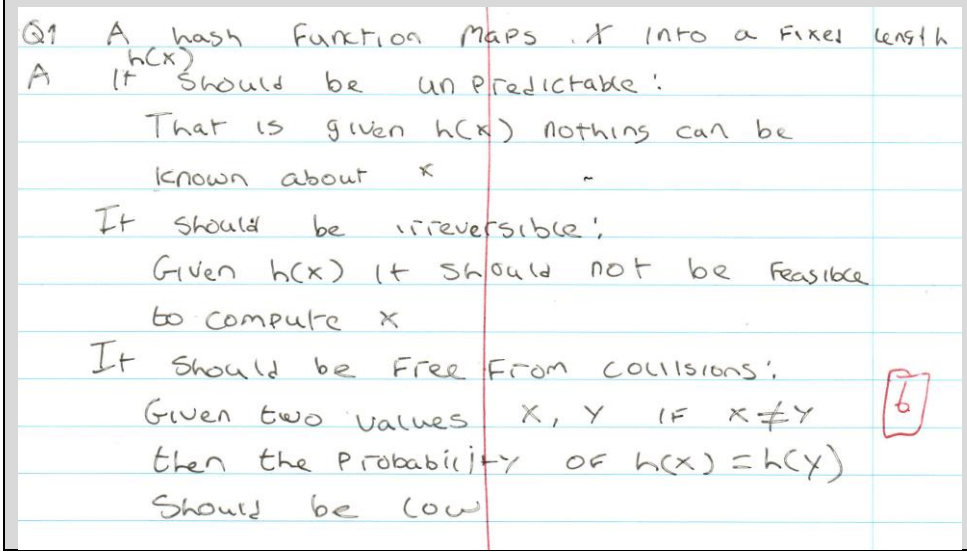
1.

a. Define the properties of a one-way hash function. (6 marks)

Answer

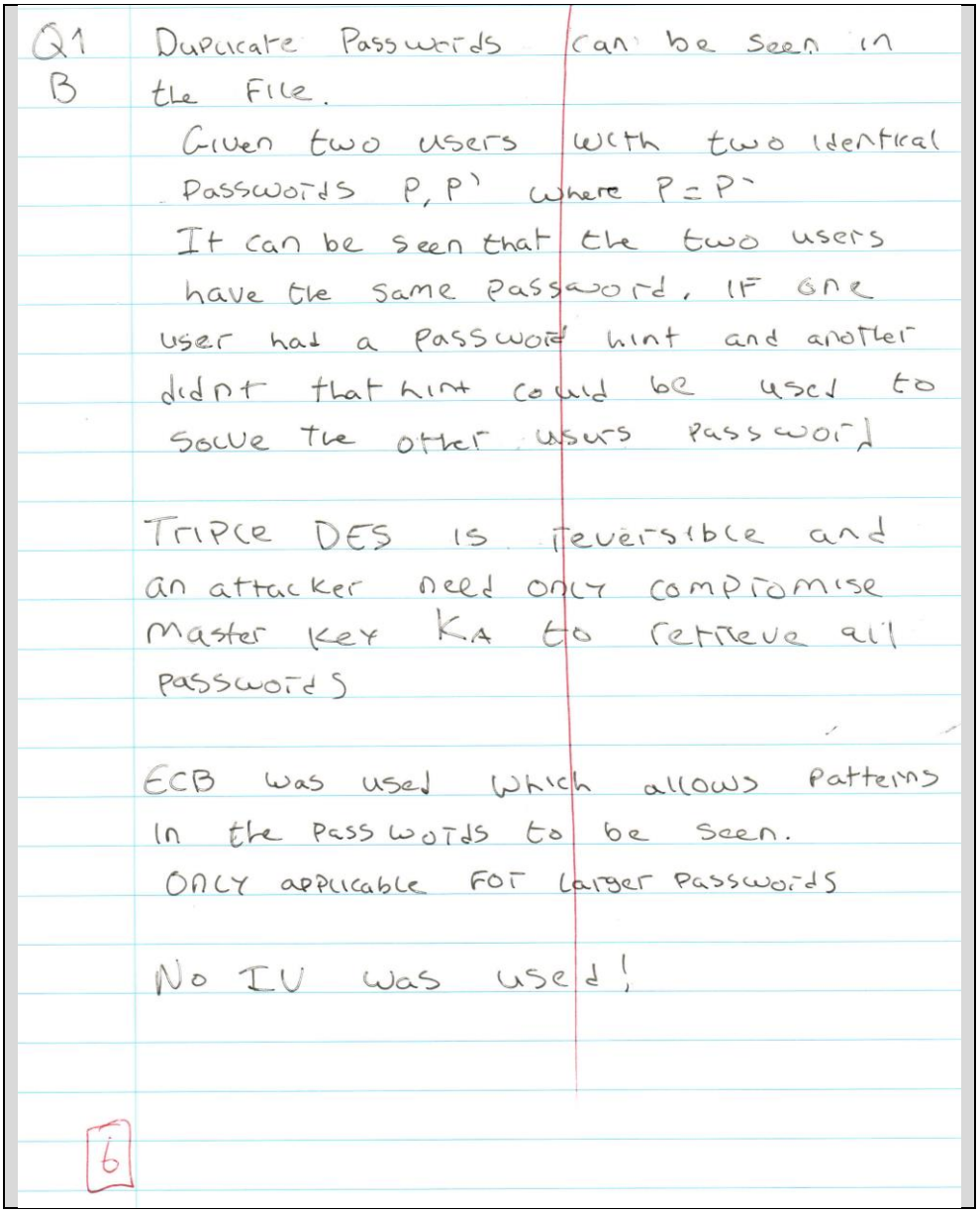
A hash function h maps arbitrary length value x to fixed length value y such that:

- Hard to reverse. Given value y not feasible to find x with y = h(x).
- Collision freeness. Hard to find values x, x' such that h(x) = h(x').
- Unpredictability. The hash value h(x) does not give any information about any part of its operand x.



b. Following an intrusion at Adobe (October 2013), attackers gained access to a user password file. It is believed that each password p was stored in encrypted form in the file as $E^{ecb}_{des}(K_A, p)$ using triple DES (ECB mode) where K_A is a secret Adobe master key. Describe two security weaknesses of this scheme. (6 marks)

Answer



Q1 B

Duplicate Passwords can be seen in the File.

Given two users with two identical Passwords P, P' where P = P'

It can be seen that the two users have the same password, IF one user had a password hint and another didnt that hint could be used to solve the other users password

Triple DES is reversible and an attacker need only compromise master key K_A to retrieve all passwords

ECB was used which allows patterns in the passwords to be seen.

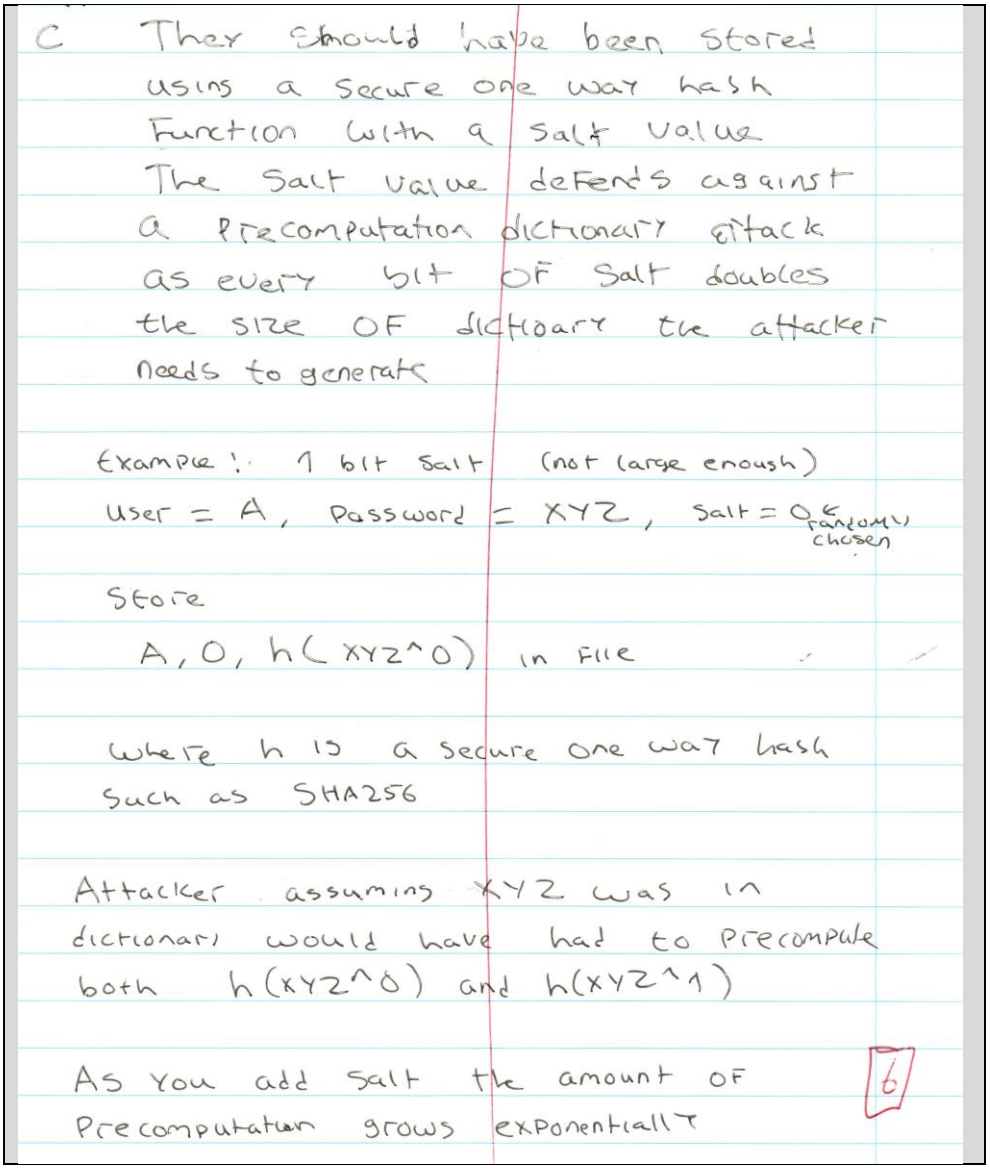
ONLY applicable FOR larger passwords

No IV was used!

6

c. Continuing Question 1 (b), describe how the passwords should have been stored and explain how your scheme defends against a pre-computation dictionary attack. (6 marks)

Answer



c They should have been stored using a secure one way hash Function with a salt value The salt value defents against a Precomputation dictionary attack as every bit OF salt doubles the size OF dictionary the attacker needs to generate

Example: 1 bit salt (not large enough)

User = A, Password = XYZ, Salt = 0 (randomly chosen)

Store

A, 0, h(XYZ^0) in File

where h is a secure one way hash such as SHA256

Attacker assuming XYZ was in dictionary would have had to Precompute both h(XYZ^0) and h(XYZ^1)

As you add salt the amount OF Precomputation grows exponentially

6

d. The following Java code generates a symmetric cipher based on a random session key.

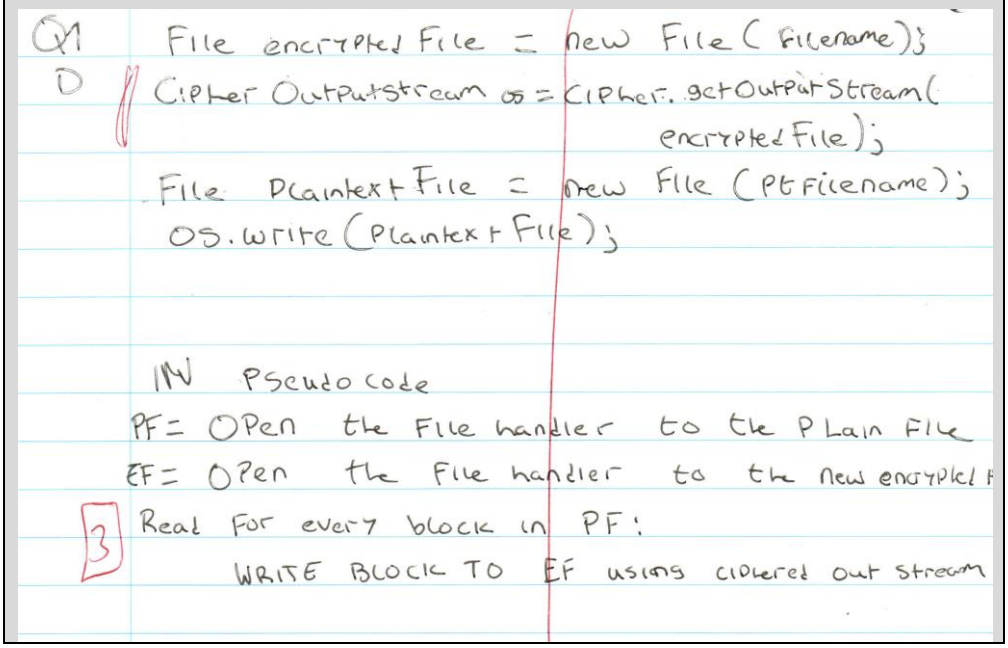
```
KeyGenerator kg= KeyGenerator.getInstance("DES");
kg.init(new Random(0));
SecretKey key= kg.generateKey();
Cipher cipher= Cipher.getInstance("DES/ECB/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE,key);
```

Give a Java code fragment that encrypts the contents of a file using this key. (6 marks)

Answer ???

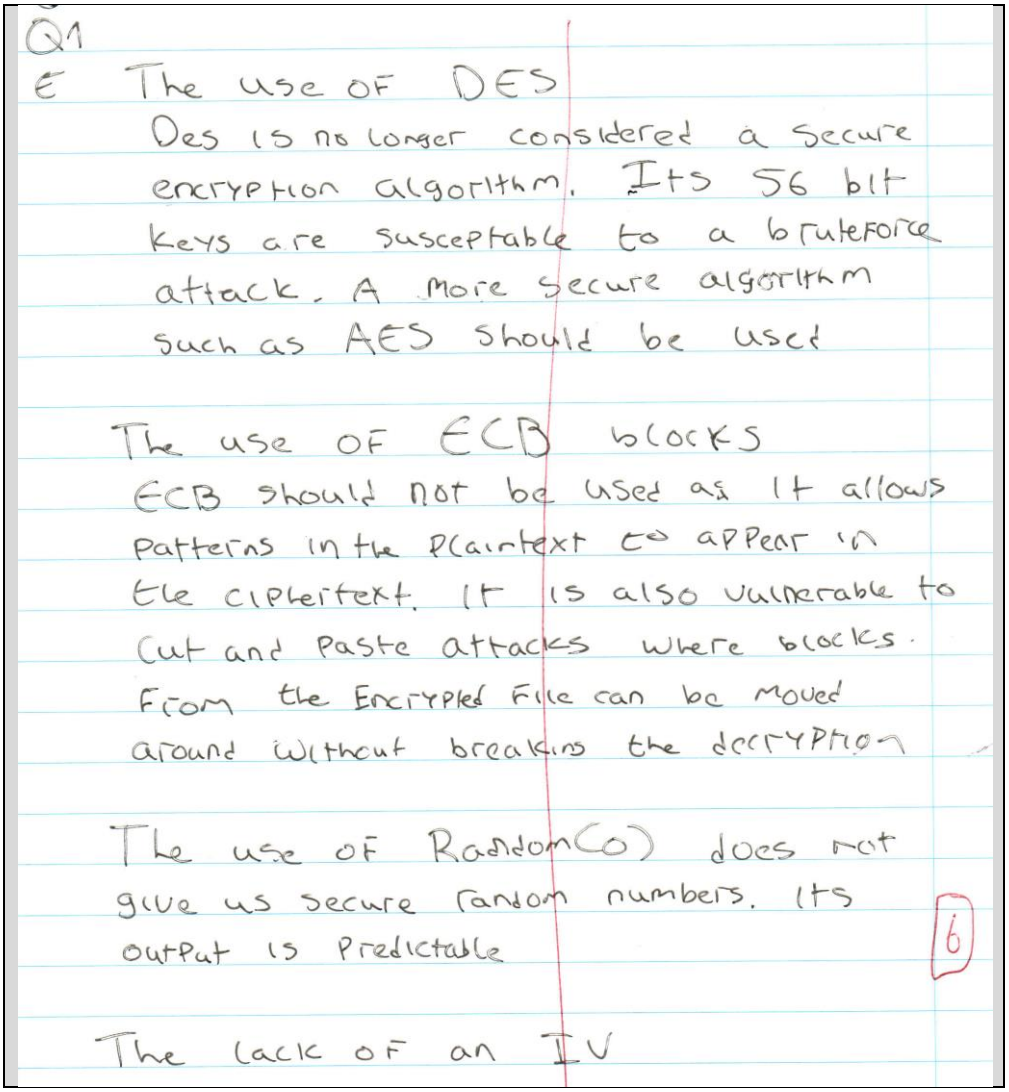
```
//creating file output stream to write to file
try(FileOutputStream fos = new FileOutputStream(fname+".des")){

//creating object output stream to write objects to file
ObjectOutputStream oos = new ObjectOutputStream(fos);
```

```
oos.writeObject(key);  //saving key to file for use during decryption

//creating file input stream to read contents for encryption
try(FileInputStream fis = new FileInputStream(fname)){

//creating cipher output stream to write encrypted contents
try(CipherOutputStream cos = new CipherOutputStream(fos,
                                                    cipher)){
int read;
byte buf[] = new byte[4096];

while((read = fis.read(buf)) != -1)  //reading from file
        cos.write(buf, 0, read);  //encrypting and writing to file
```



e. Identify and explain any security vulnerabilities in the code in Question 1(d) above. (6 marks)

Answer ???



Q1

e The use of DES

Des is no longer considered a secure encryption algorithm. Its 56 bit keys are susceptable to a bruteforce attack. A more secure algorithm such as AES should be used

The use of ECB blocks

ECB should not be used as it allows patterns in the Plaintext to appear in the ciphertext. It is also vulnerable to cut and paste attacks where blocks. From the Encrypted File can be moved around without breaking the decryption

The use of Random() does not give us secure random numbers. Its output is Predictable

6

The lack of an IV

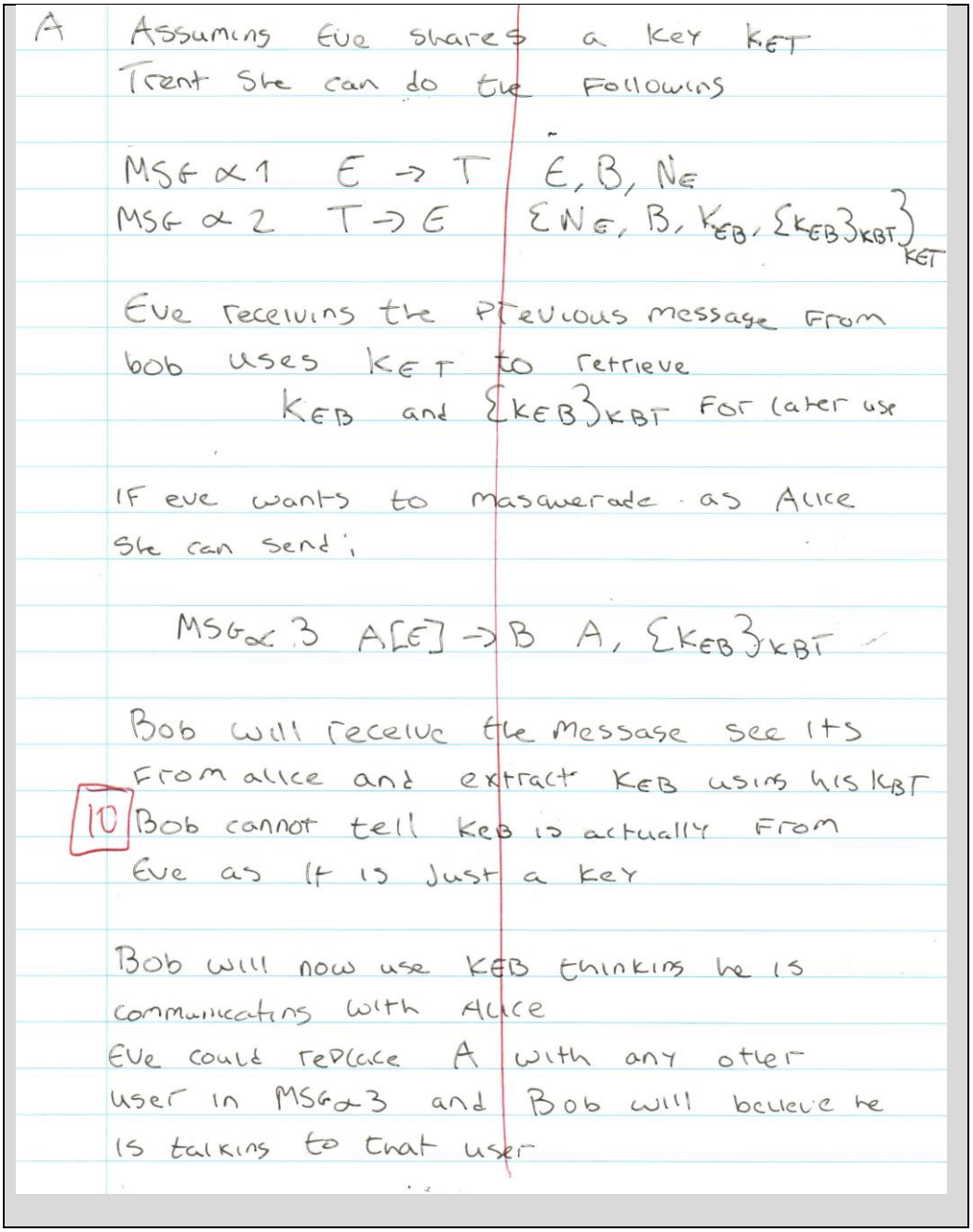
2. Consider the following Needham-Schroeder style authentication protocol, whereby initiator A asks Authentication Server Y for a session key K_{AB} that it can use with service B.

$$\begin{array}{lll} \text{Msg1} & A \rightarrow T: & A, B, N_A \\ \text{Msg2} & T \rightarrow A: & \{N_A, B, K_{AB}, \{K_{AB}\}_{K_{BT}}\}_{K_{AT}} \\ \text{Msg3} & A \rightarrow B: & A, \{K_{AB}\}_{K_{BT}} \end{array}$$

Principles A and B share long-term secret keys K_{AT} and K_{BT} with server T, respectively; N_A is a nonce and $\{\ldots\}_K$ denotes symmetric key encryption with secret key K.

a) Describe an attack on the protocol whereby Eve can masquerade as A to B. (10 marks)

Answer



A Assuming Eve shares a key K_{ET} Trent She can do the Followins

$MSG\alpha 1 \quad E \rightarrow T \quad E, B, N_E$

$MSG\alpha 2 \quad T \rightarrow E \quad \{N_E, B, K_{EB}, \{K_{EB}\}_{KBT}\}_{KET}$

Eve receiving the previous message From bob uses K_{ET} to retrieve K_{EB} and $\{K_{EB}\}_{KBT}$ For later use

IF eve wants to masquerade as Alice She can send;

$MSG\alpha 3 \quad A[E] \rightarrow B \quad A, \{K_{EB}\}_{KBT}$

Bob will receive the message see its From alice and extract K_{EB} using his K_{BT}

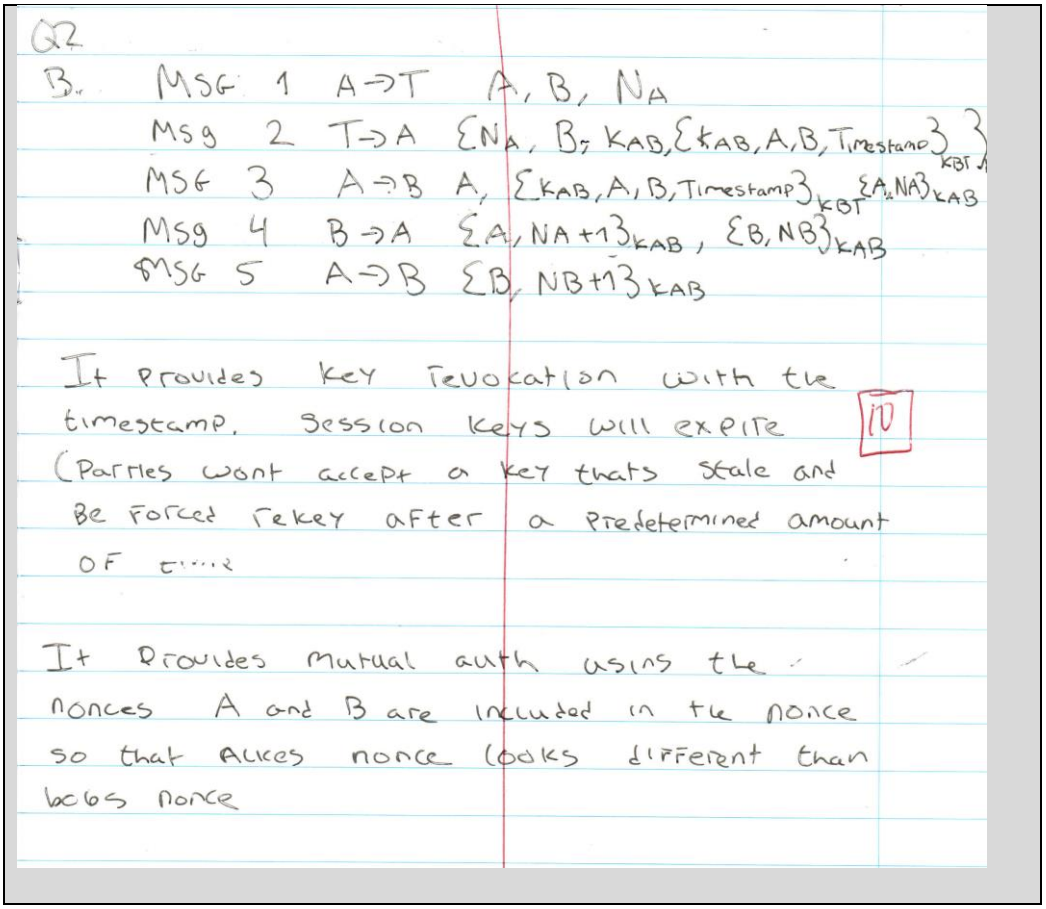
10 Bob cannot tell K_{EB} is actually From Eve as it is just a key

Bob will now use K_{EB} thinking he is communicating with Alice

Eve could replace A with any other user in $MSG\alpha 3$ and Bob will believe he is talking to that user

b) Revise the protocol so that: it eliminates the vulnerability in Question 2(a): provides mutual authentication between A and B and supports key revocation in the event that K_{AT} is compromised. (10 marks)

Answer



Q2

B. MSG 1 A→T A, B, N_A

Msg 2 T→A $\{N_A, B, K_{AB}, \{K_{AB}, A, B, Timestamp\}_{KBT}\}_{KAT}$

MSG 3 A→B A, $\{K_{AB}, A, B, Timestamp\}_{KBT}$ $\{A, NA\}_{KAB}$

Msg 4 B→A $\{A, NA+1\}_{KAB}$, $\{B, NB\}_{KAB}$

MSG 5 A→B $\{B, NB+1\}_{KAB}$

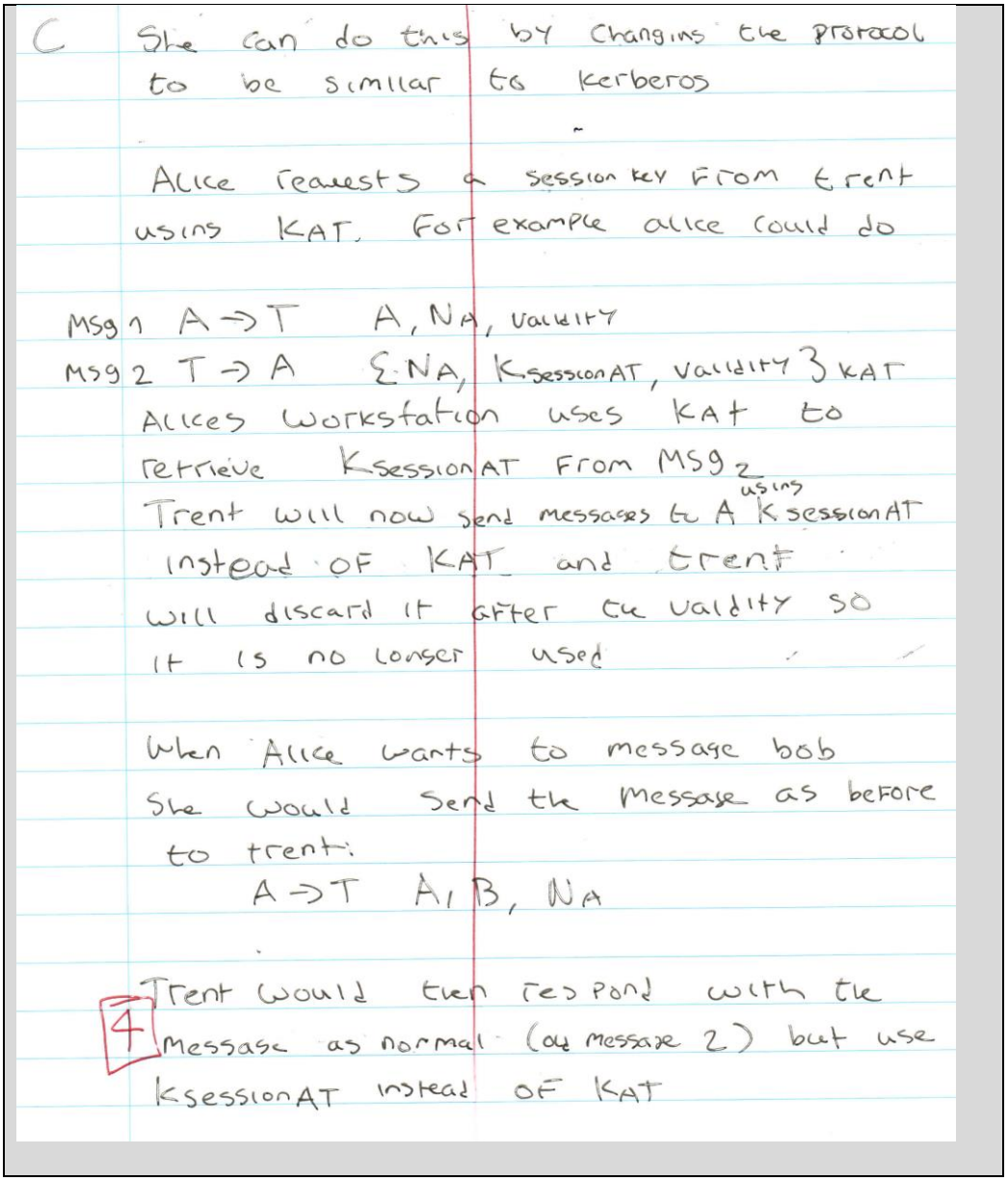
It provides key revocation with the timestamp. Session keys will expire (Parties wont accept a key thats stale and be forced rekey after a predetermined amount of time

10

It Provides mutual auth using the nonces A and B are included in the nonce so that Alices nonce looks different than bobs nonce

c) Alice logs into the workstation corresponding to Principle A and K_{AT} is determined by her password. Alice does not want to give her password every time she uses the protocol to request services, however, she is concerned about the workstation storing long-term key K_{AT} for the duration of her login session. Describe how the protocol can be revised to provide single-sign-on for Alice while addressing her password security concerns. (5 marks)

Answer



C She can do this by changing the protocol to be similar to kerberos

Alice requests a session key from trent using KAT. For example alice could do

Msg 1 A → T A, N_A, validity

Msg 2 T → A $\{N_A, K_{sessionAT}, validity\}_{KAT}$

Alices workstation uses KAT to retrieve $K_{sessionAT}$ from Msg 2

Trent will now send messages to A using $K_{sessionAT}$ instead of KAT and trent will discard it after the validity so it is no longer used

When Alice wants to message bob she would send the message as before to trent:

A → T A, B, N_A

Trent would then respond with the 4 message as normal (as message 2) but use $K_{sessionAT}$ instead of KAT

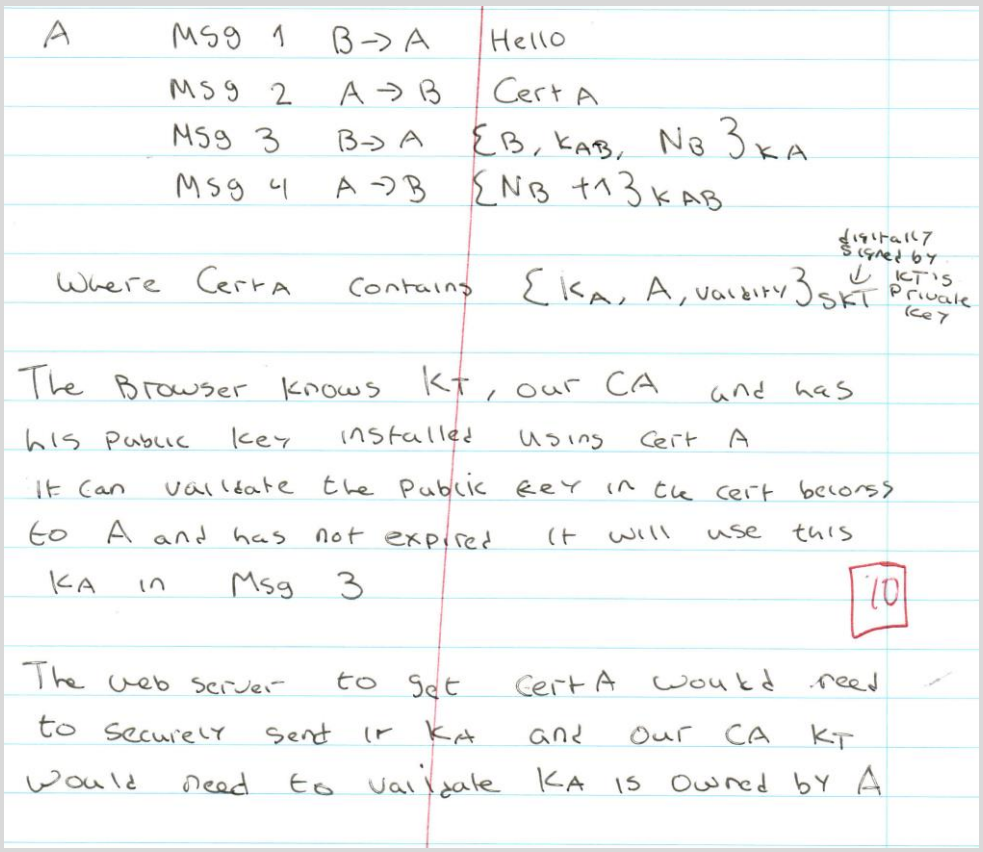
3. The following SSL-style protocol fragment establishes a secure connection between browser B and web-server A:

$$\begin{array}{lll} \text{Msg 1:} & B \rightarrow A & : \{B, K_{ab}, N_A\}_{K_A} \\ \text{Msg 2:} & A \rightarrow B & : \{N_B + 1\}_{K_{ab}} \end{array}$$

where K_A is the public key owned by A, K_{ab} is a symmetric key proposed by A and N_B is a nonce. In a Protocol Msg 1, {…}K_{ab} denotes symmetric key encryption in Protocol Msg 2.

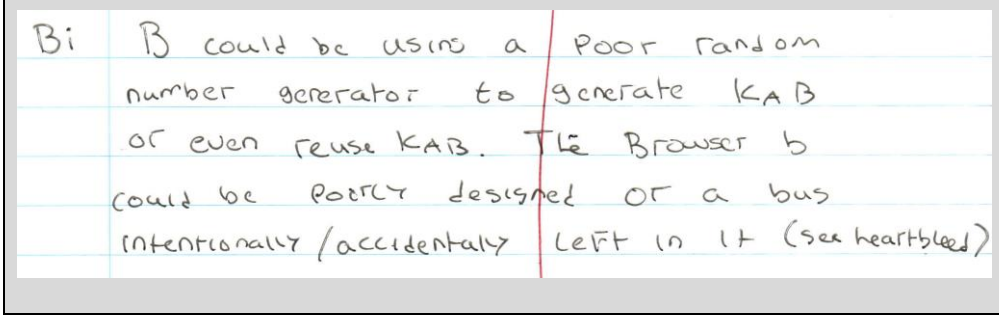
a) Explain how the protocol should be extended to support public key certificates. Your answer should include a revision of the protocol, description certificate)s) content and how it is used by the browser / web server. (10 marks)

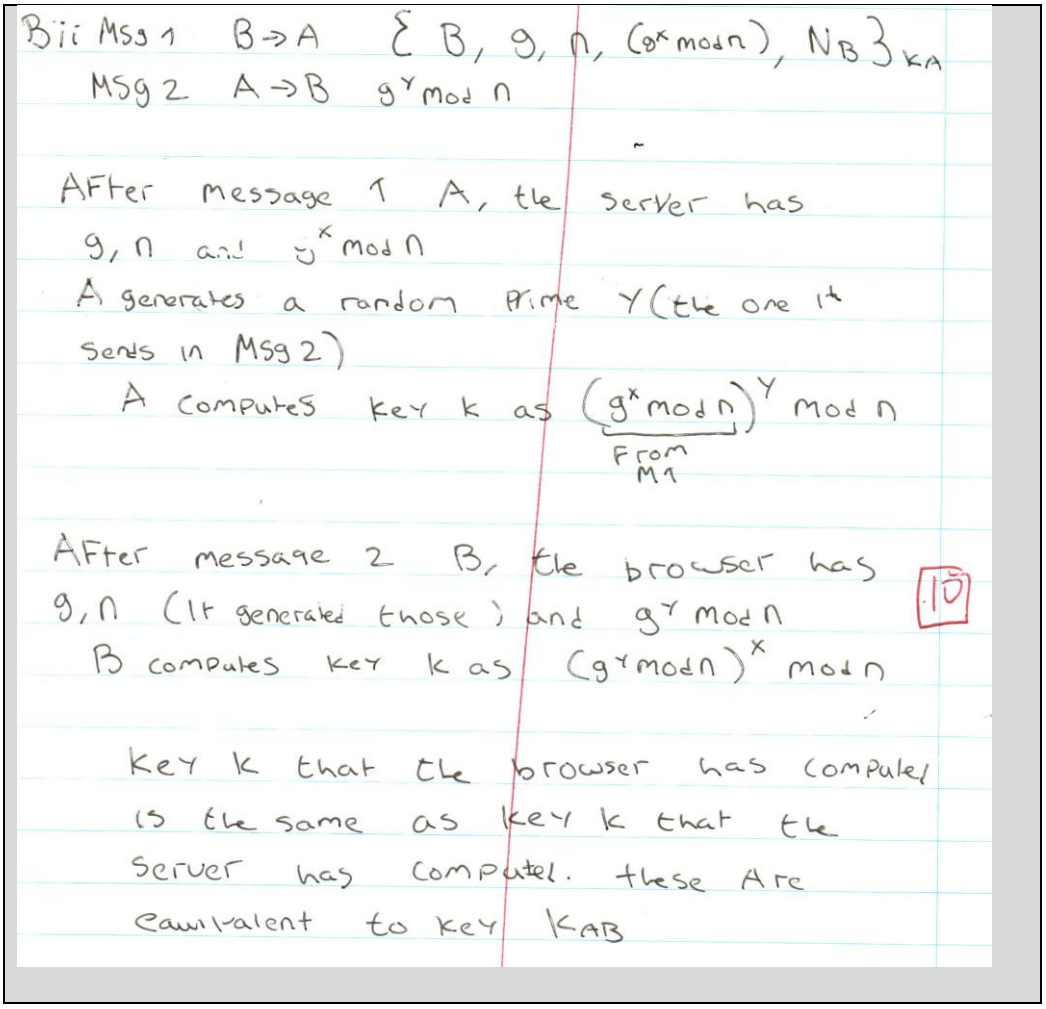
Answer



b) The protocol assumes that B is competent to generate a good session key K_{ab}. Give an example of why this might not be the case. Revise the protocol so it uses a Diffe-Hellman key exchange to establish the session key K_{ab}. (10 marks)

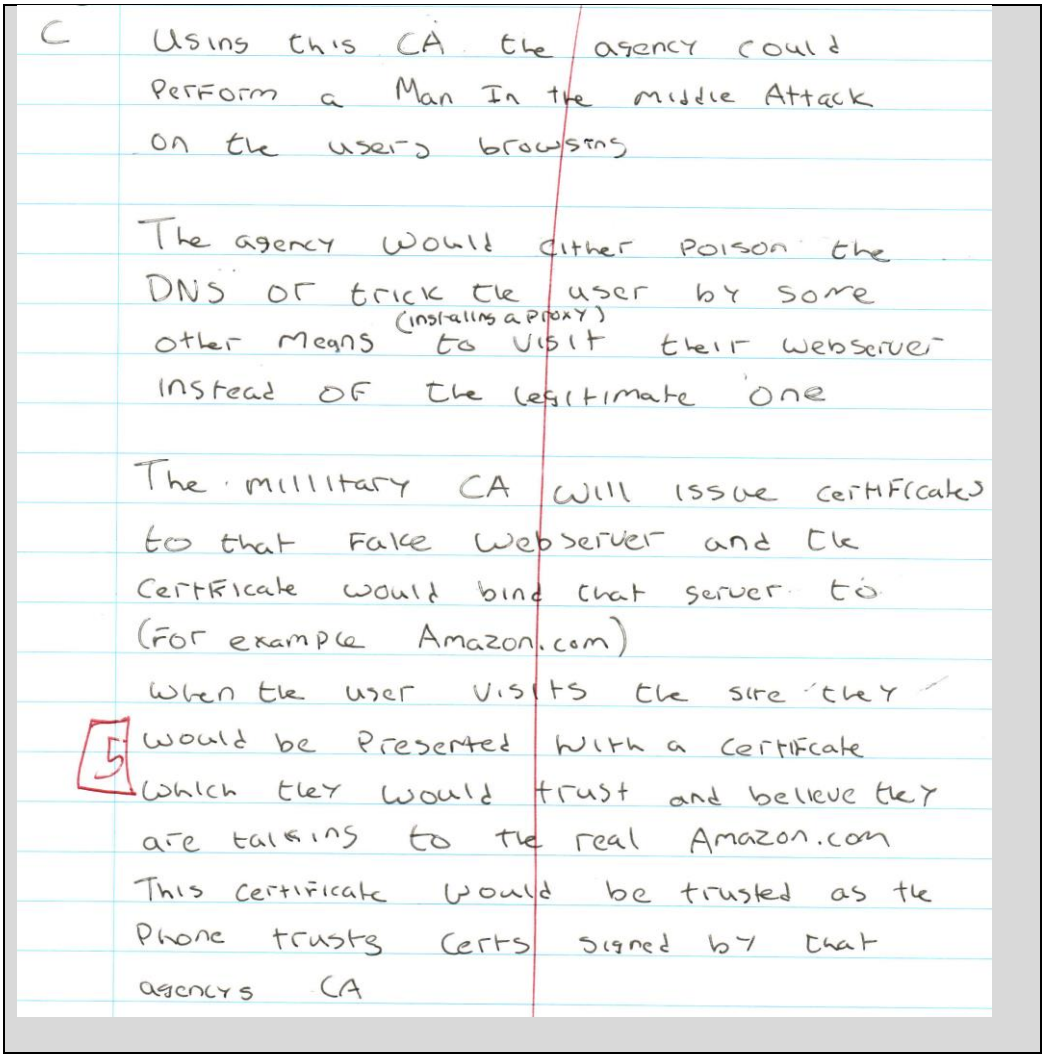
Answer





c) Apple iOS comes with a pre-installed trusted Certificate Authority (CA) certificate from a foreign military agency. Describe how this agency might spy on a user's secure (HTTPS) web browsing. (5 marks)

Answer



c

Using this CA the agency could perform a Man In the middle Attack on the users browsing

The agency would either poison the DNS or trick the user by some other means (installing a proxy) to visit their webserver instead of the legitimate one

The millitary CA will issue certificates to that Fake Webserver and the certificate would bind that server to (for example Amazon.com)
When the user visits the site they would be presented with a certificate which they would trust and believe they are talking to the real Amazon.com
This certificate would be trusted as the Phone trusts certs signed by that agencys CA

5