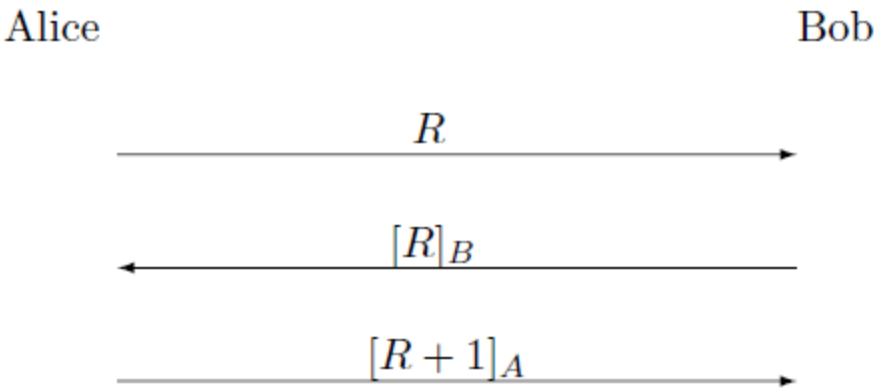
CS5285 PS2

Gerhard Hancke

Question 1

- Consider the following protocol



- (a) Explain why this protocol is not secure.

Question 1(a)

- Solution:

Alice is not authenticated as the message from here is not fresh – there is never a challenge by Bob.

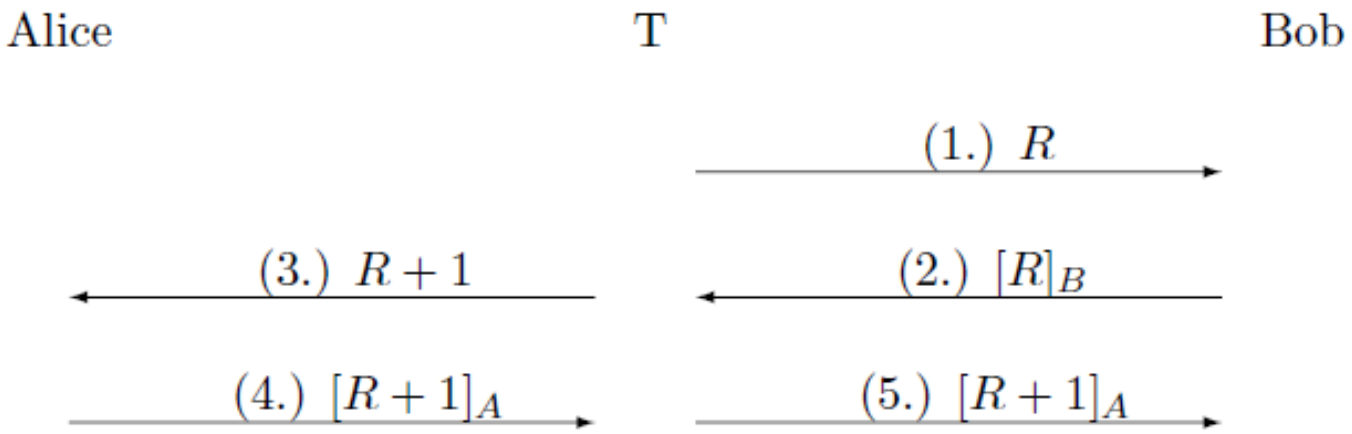
So an eavesdropper T listens to the communication between Alice and Bob, and stores a transcript, i.e. $(R, [R]_B, [R+1]_A)$. Later, T impersonates Alice to Bob by ***replaying*** this transcript.

This attack works if Bob doesn't remember/store the transcripts of previous executions of the protocol.

Note that in this attack T doesn't need to interact with Alice in order to impersonate her.

Question 1(a) con't

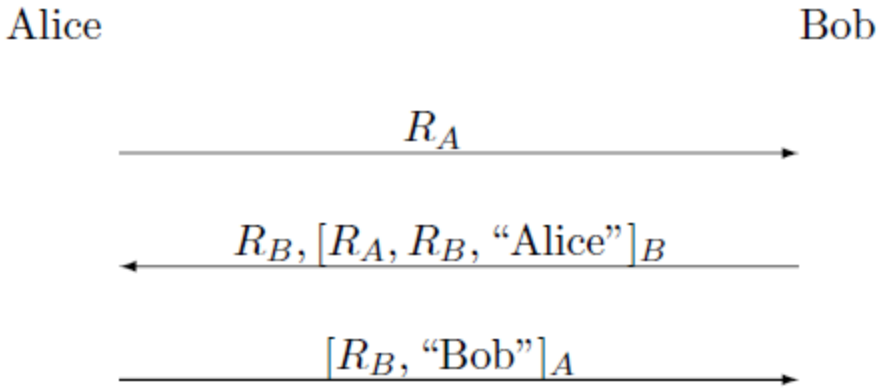
A second attack is when T interacts with Alice when impersonating her (**reflection, MITM**):



Question 1(b)

- Modify the protocol such that it supports mutual authentication. Your modification cannot add any encryption, digital signature or new message flow.

Solution: To prevent the replay attack, Alice and Bob need to choose their own challenges (nonces) and append their counterpart's identity to the nonces to be signed so that the recipient would abort the execution if the included identity is not his/hers.



Question 2

a+b) Recover the passwords in file1, file 2, file 3

- Search for salt/pass with MD5 five characters (lower, upper, numeric)
- File 1 5-digits (A-Z,a-z,0-9)
  - pswd3, L0v3Y, X4286, MyD0g, CityU
- File 2 5-digits with 8-bit SALT
  - pswd3, L0v3Y, X4286, MyD0g, CityU
- File 3 6-digits (A-Z,a-z,0-9)
  - psswrd, 1L0vEU, CS4286, MyD0g8, CityU1

Question 2

c) Not that noticeably different- because we are not building an entire dictionary. There is only 5 salts so hashcat looks for all password combinations with the 5 salts given. So instead of searching space of 62^5.255 we are only searching 62^5.5.

If we had much entries with 255 unique salts then we would be looking at getting the full extra 8 bit dictionary space.

d) Should be noticeably a bit longer to find.

Question 3

- Consider the following attacks to internet security and describe how each is countered by a particular feature of SSL. Assume the size of the secret key used by SSL is 128 bits.
- (a) Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.

Solution: When the size of the secret key used by SSL is 128 bits, the number of possible keys is $2^{128} \approx 3.4 \times 10^{38}$. Brute force effort 2^{127} too much

Q3(b)

- Known-Plaintext Dictionary Attack: Many messages contain predictable plaintext, such as the ‘HTTP GET’ command. An attacker constructs a dictionary containing every possible encryption of the known-plaintext message. The attacker can look up the ciphertext in the dictionary to determine the secret key.

Solution: When the size of the secret key used by SSL is 128 bits, it takes at least $2^{128}/8$ bytes $\approx 4.25 \times 10^{31}$ GB to completely store all these possible keys in a table. So using this kind of attack will take huge amount of memory and computing time.

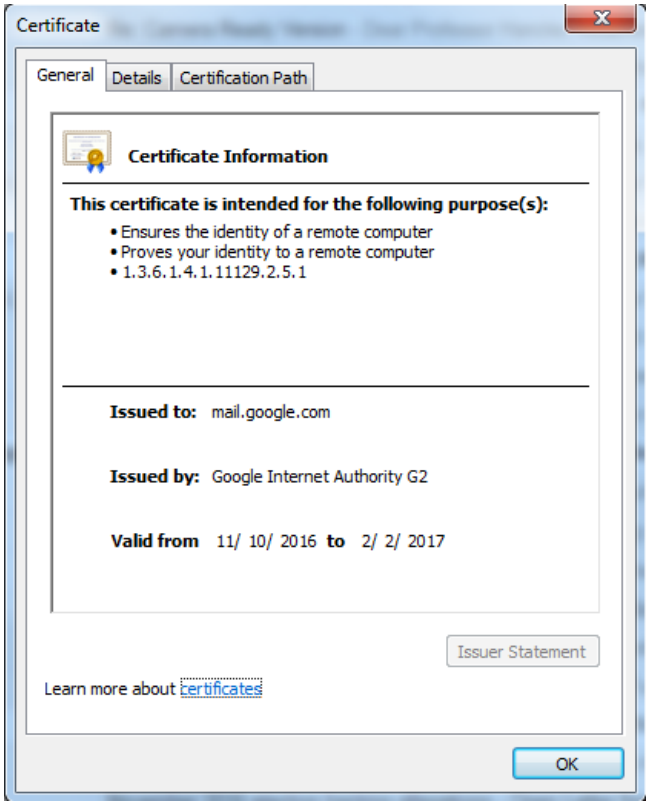
Q3(c)

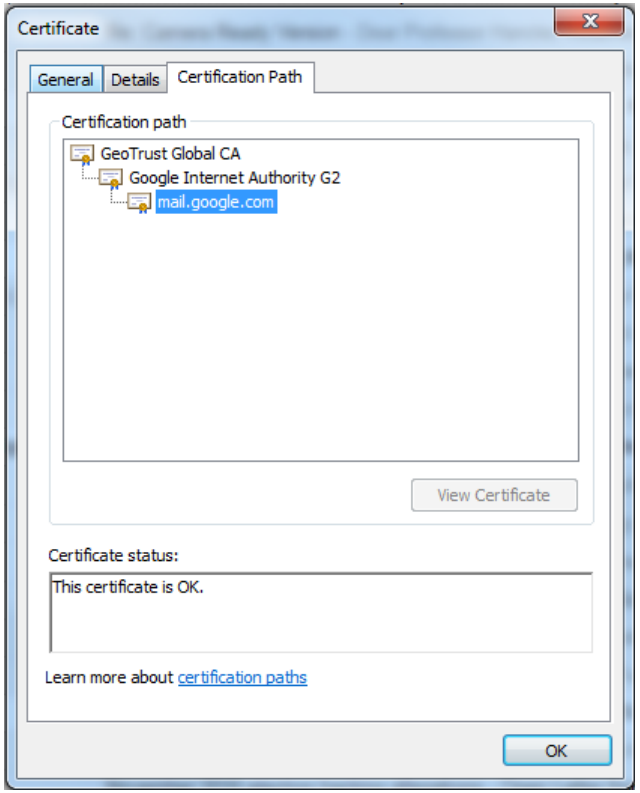
(c) Replay Attack: Earlier SSL messages are replayed.

Solution: When a session ends in SSL, the secret key used by the session will be discarded. New secret key and random numbers (nonces) will be generated when a new session is started, and the chance of collisions of the secret keys and random numbers (nonces) will be negligible.

Question 4(a)

- Find out who issued the certificate for https://mail.google.com and how long the certificate will be valid.
- Solution:





Q4(b)

- Find out or estimate how many certificates (approximately, no need to count them explicitly) your browser contains.

- Solution: Example - IE on Windows: +- 300 certificates (these certificates are common to many Windows applications).

Q4(c)

What is the significance of a CA certificate being contained in the browser?

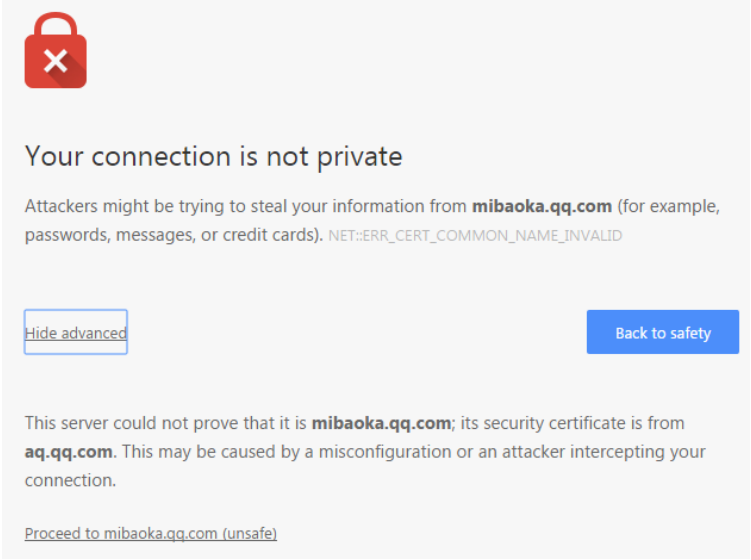
Solution:

The special property of CA certificates included in a web browser is that the web browser implicitly trusts any certificate signed by one of these CAs.

Q4(d)

- Use a web browser to connect to the URL https://mibaoka.qq.com/. You should get an error that there is a problem. What is the problem of this connection?
- Solution:

The error shows that the security certificate presented by this website was issued for a different website's address: aq.qq.com.



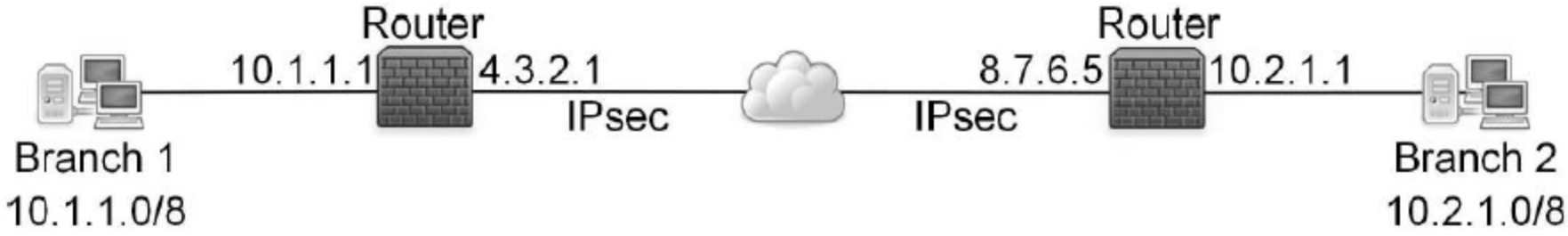
Q4(e)

- The identity of the certificate for the two questions above is a DNS hostname. Certificates can also be used for signing and encrypting email. For a certificate used for email, what identifier would be used as the identity in the certificate?

Solution: Certificates used for encrypting or signing emails bind a public key to an *email address*

Question 5

Imagine two branches of a corporate network are connected through the Internet. Specifically, each of the two branches has a router facing the Internet, communicating with the router of the other branch over IPsec.



Q5(a)

- If ESP is used to secure the communication between the two routers, which mode will be used, transport mode or tunnel mode? Why?

Solution: Tunnel mode should be used because the routers are connecting two networks.

Q5(b)

The network is setup such that two nodes from the two branches can communicate transparently. Imagine node 10.1.1.5 from branch 1 is sending a packet to node 10.2.1.6 from branch 2. Describe in detail the steps of how the packet travels between the two nodes and how it is encapsulated and decapsulated on the way.

Solution: The following steps will take place as a packet travels between the two nodes:

(1) Node 10.1.1.5 prepares a packet with the address 10.2.1.6 as the destination address and forwards it to the router of its network (the default gateway for the node).

Q5(b) con’t

(2) The router receives the packet on its internal interface 10.1.1.1 and realises that it is destined for a node in the network of branch 2. It therefore adds the ESP header, trailer and auth and then encapsulates the packet into an outer packet, with the address 4.3.2.1 as the source address (the external address of the router of branch 1) and the address 8.7.6.5 as the destination address (the external address of the router of branch 2). The packet is then sent over the Internet to the router of branch 2.

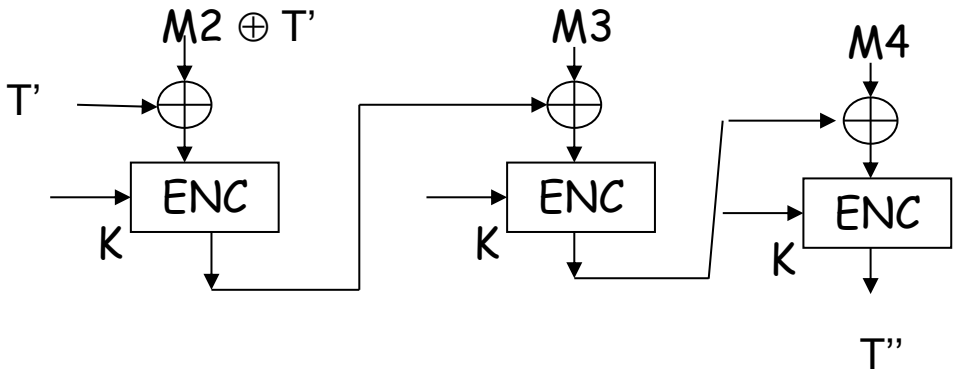
(3) The router of branch 2 receives the packet on its external interface. It decapsulates the packet, checks the authentication trailer and decrypts the inner packet (which still has the destination address 10.2.1.6). It then forwards the inner packet onto the internal network of branch 2.

(4) Node 10.2.1.6 receives the packet.

Q6

MACs: M'(M0,M1) = T',
M'' (M2,M3,M4) = T''

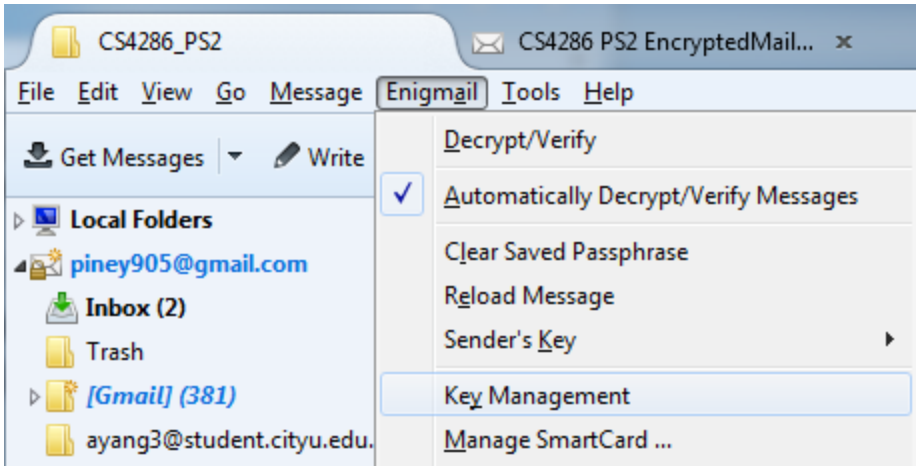
Choose M = M2 ⊕ T'
M'''= M0,M1,M2 ⊕T',M3,M4

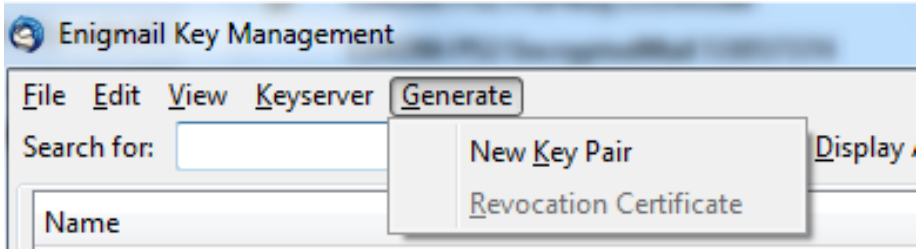


As we start the MAC of M''' after M0 and M1 our results is T'

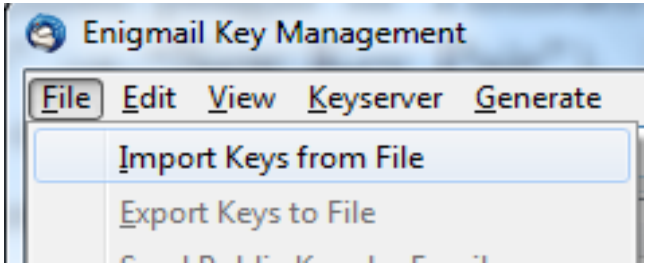
With our choice of M, what we feed into the ENC is M2. This is the same as doing the MAC for M''. So we end up with same MAC tag T''/

Question 7 sol





(a)



(b) Download the tsgexercise_cert.asc and import it into Enigmail

(c) Send me some text encrypted with the downloaded public key first and then signed with your own private key as well, rather than only send me your public key.

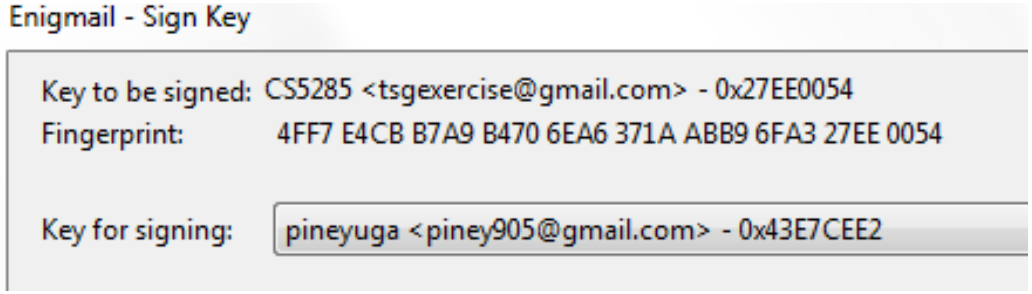
Q8-solution

- Indications

1 Mutually certifying your PGP keys. If you have no partner, you can create two PGP key pairs with different accounts.

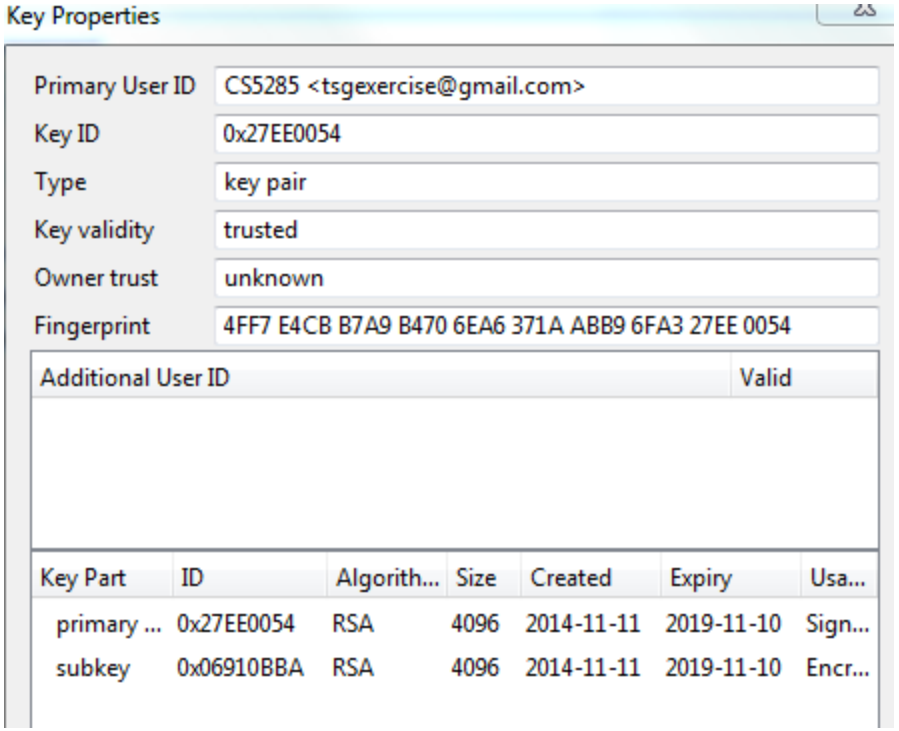
Q8-sol con't

2 Then sign your partner's public key with your own private key.



Use pineyuga's private key to sign CS5285's public key

We can see the result:



If you are happy, you can ask as many friends as you can to sign your public key.

The end!

?

Any questions…