Computer and Network Security – Exercise no. 2

Submit in Pairs/Single to mailbox 19 by 21/12/11, 2:00 p.m.

1. (a) To communicate between themselves securely, the leaders of the European Union decided to use PGP web of trust.
   Sarkozy always trusts Merkel and Cameron.
   Sarkozy usually trusts Zapatero, Monti, Kenny, Rutte.
   Papademos always trusts Thorning-Schmidt.
   Sarkozy signed certificates for Cameron, Kenny, Tusk, and Katainen.
   Cameron signed certificates for Rutte, Putin, Faymann and sent them to Sarkozy.
   Monti signed certificates for Zapatero, Nečas, Thorning-Schmidt, and sent them to Sarkozy.
   Kenny signed certificates for Merkel, Cameron, Monti, Nečas, and sent them to Sarkozy.
   Merkel signed certificates for Papademos and Monti, and sent them to Sarkozy.
   Papademos and Thorning-Schmidt signed certificates for each other, and sent them to Sarkozy.
   Faymann signed a certificate for himself and sent them to Sarkozy.
   Rutte signed a certificate for Thorning-Schmidt, Nečas, and Monti, and sent them to Sarkozy.

   Assume that if the trust is not defined (i.e., A's trust on B is not defined), then it does not exist (i.e., A does not trust B).
   i. What keys Sarkozy finds legitimate when $X = 1$ and $Y = 2$?
   ii. What keys Sarkozy finds legitimate when $X = 1$ and $Y = 3$?

   (You may wish to construct the public key ring in a graph like we've seen in class).

   (b) In PGP, for the computation of the Key Legitimacy, only signatures which were made by a legitimate key are considered. Assume that for the computation of Key Legitimacy we would have used all the certificates, including those which were made by illegitimate keys. We shall see now that this model is insecure.
   Independently of the previous question and under the new model:
   Assume that Cvetković trusts Reinfeldt, and he knows Reinfeldt's public key as a legitimate one. Also, Cvetković does not trust Sócrates, but he knows his public key as a legitimate one. Show how Sócrates can send Cvetković a document with the name of Obama such that Cvetković indeed believe that Obama sent him the document.
   Assume that $X = 1$.

2. On FaceCook, users can send messages to other users. A new user A registers with his personal information. Then, when he wishes to communicate with B which is already a user, he can do so via the website. The message is sent to the servers of FaceCook, and when B enters the website, he receives the stored message.

   It is known that:

- All user names in FaceCook are unique.
- Any user can view the personal information of all users and to communicate with them.
- The website is secure, and the only details a user can alter are his own.
- All the loaded details are available on the servers of FaceCook.

The users of FaceCook were afraid that the owner of FaceCook (Dark Cuzkerberg) could read their messages, and analyze them for advertisements. Thus, they decided to use public key cryptography to protect their communications. Each user installs on his computer a software that does the followings:

- The software securely generates an RSA public key (and private key) 2048 bits long.
- The software adds the public key to the personal details of the user on FaceCook (this could also be done manually by the user).
- When A wishes to communicate with B, the software takes B's public key details from FaceCook, encrypts the message, and sends it to B. On B's side, once he connects, he receives the encrypted message, and the software decrypts it using the private key.

(a) Is it possible that two users of the site will have the same public key?
If so, explain how. Otherwise, explain why not.

(b) Does the suggested method protect the privacy of the messages?
If so, explain how. Otherwise, show an attack.

(c) Can A and B who do not know each other and never met, can verify that they are indeed the owners of the public key found on the website, without any help from a third party or the website? If there is such a system, explain it. Otherwise, explain why it is impossible to have such a system.

3. In the "Hacking for Senior Citizens" there are N students, who wish to communicate with each other. To protect the messages, it was decided to add a MAC tag for integrity and authenticity. The used MAC is the secure HMAC-SHA1 (i.e., it cannot be broken if the adversary does not know the key).

(a) For efficiency reasons, it was decided that all students will share the same key K. Explain why this method offers insufficient security.

(b) Following the failure of the previous method, it was decided to use N different keys, $K_1, K_2, \ldots, K_N$. Where the user i obtains the $N-1$ keys, $K_1, K_2, \ldots, K_{i-1}, K_{i+1}, \ldots, K_N$.

i. Suggest a method such that student i can send to student j an authenticated message using HMAC-SHA1, such that no other single student can alter (without being caught). Show that your method is indeed secure.

ii. Moishe received an authenticated message from Rachel, asking him to send his homework to Hershel and Bella. When Moishe met Rachel in the classroom, she claimed that she did not send this message. Assuming Rachel is not lying, show how such a situation might have happened.

Due to the failure of the previous methods it was suggested to use RSA signatures. The students decided to pick the lecturer as a CA, and they all trust her (as Eve is known to be an honest lecturer), and know her public key for encryption Pub_{EveEnc} and for signature Pub_{EveSig}. Eve also knows all the students.

The generation of certificates is as follows:

- Each student meets with Eve in her office, according to the alphabetical order of the names of the students.
- The student meets with Eve, and gives her his (or hers) public key.
- Eve copies the public key of the student to her computer, and after checking the ID number of the student, issues a certificate. Eve does not issue certificate for students whose identity was not proved.
- Eve issues a certificate with the identity of the student and his (or hers) public key, and signs it with Pri_{EveSig}. The certificate is then loaded to Eve's private web server which is secure and authenticated (all communications with this server are secure and authenticated).
- The next student enters the office, and the process repeats.

After obtaining the certificates, the students send each other messages using their private keys with **a secure** signature algorithm for authentication.

For the next questions, assume that all communications is public (i.e., not encrypted, only authenticated) including the ones in Eve's office.

(c) Eve asked the students to submit their homework through email in an encrypted and signed method, i.e., a student with private key Pr_A will send $ID_A, E_{Pub_{EveEnc}}(M), Sig_{Pr_A}(M)$, where E is a secure RSA encryption, M is the homework, and Sig is a secure signature algorithm.

Ahron was the first student to receive his certificate from Eve, and was also the first one to submit his homework using the new method by sending:
$ID_{Ahron}, E_{Pub_{EveEnc}}(M), Sig_{Pr_{Ahron}}(M)$.
Show how Baruch, by planning ahead could copy Ahron's homework M without Ahron's approval. In other words, show how Baruch can send the message:
$ID_{Baruch}, E_{Pub_{EveEnc}}(M), Sig_{Pr_{Baruch}}(M)$.

Following the problems of the previous solution, it was suggested to use a new method. Each student accepts a student number between 1 and N. The new certificate issuing procedure is:

- Each student meets with Eve in her office, according to the order of the student numbers.
- The student meets with Eve, and gives her his (or hers) public key.
- The student presents his (or hers) RSA signature on his (or hers) assigned student number. Namely, the ith student with public key (n_i, e_i) and secret key d_i presents to Eve $y_i = i^{d_i} \bmod n_i$.

- Eve copies the public key of the student to her computer, and after checking the ID number of the student, and that $y_i^{e_i} = i \bmod n_i$ issues a certificate. Eve does not issue certificate for students whose identity was not proved or whose signature check fails.
- Eve issues a certificate with the identity of the student, the student number, and his (or hers) public key, and signs it with Pri_{EveSig}. The certificate is then loaded to Eve's private web server which is secure and authenticated (all communications with this server are secure and authenticated).
- The next student enters the office, and the process repeats.

(d) What is the main difference between this process and the previous process.

(e) Despite the new process, one of the students succeeded in cheating and submitting someone else's homework again. This was done without the cooperation of anyone else. Explain how this was done.

4. In this question, you are requested to compute a Diffie-Hellman key. For this purpose, we shall use $p = 44449$ and $g = 11114$.

   Usually, one first selects the secret keys, and then the public keys are computed. However, we shall start by selecting the public keys, which then will be used to compute the secret keys, and then the joint key.

   Let y_1 be digits 6–9 of the ID of the first submitter, i.e., if your ID is 123456789, $y_1 = 6789$. Let y_2 be digits 2–5 of the ID of the second submitter (unless there is one, and then these are the digits of the ID number of the sole submitter).

   (a) Find x_1 for which $g^{x_1} \equiv y_1 \bmod p$ and x_2 for which $g^{x_2} \equiv y_2 \bmod p$.

   (b) Compute the Diffie-Hellman key produced by the public keys y_1, y_2.

   (c) Given the public key $y = 11113$, find its corresponding x. Explain how you succeeded to do so, despite the fact that Diffie-Hellman is secure.