SECURITY

Assignment 14, Monday, January 21, 2018
S1013793 Carlo Jessurun
S1013792 Tony Lopar
Radboud University

Teaching assistant: Joost Rijneveld

Exercise 1

A. The goal of secrecy is not achieved, since the vote is signed with the private key of the voter which means the polling station can trace what a specific voter has voted by verifying the signature.
   The goal of single-vote is achieved, since the polling station can check whether a certain certificate is sent twice.
B. PS uses his private key to recover the value of r and compute the concatenation. Then it signs it with his private key.
C. Secrecy: No, since the vote is sent in plaintext by the voter to the polling station. This means that the polling station can see what voter V has voted.
   Single-vote: Yes, since the PS can choose to only sent a message back when only one message was sent.

Exercise 2

A. The flaw is in the fact that K_{si} is sent to Alice. In the second rule Alice can retrieve the session key using her own key. This can be done, since this key is encrypted by the XOR of K_A. In XOR we can also decrypt the message using the same key. So, Alice may find the session key as follows:
   $K_A \oplus K_A \oplus K_{ASi} = 0 \oplus K_{ASi} = K_{ASi}$
   Now Alice knows the session key she can use it to retrieve the secret key from the service by using the session key to decrypt the key in the ticket.
   $K_{Si} \oplus K_{ASi} \oplus K_{ASi} = 0 \oplus K_{Si} = K_{Si}$

B. Eve can perform a man-in-the middle attack by modifying the service in the first message.
   $A \rightarrow E$: A, S_1
   $E \rightarrow TGS$: A, S_2
   $TGS \rightarrow E$: $K_A\{K_{AS2}\}, K_{S2}\{K_{AS2}\}$(= ticket)
   $E \rightarrow A$: $K_A\{K_{AS2}\}, K_{S2}\{K_{AS2}\}$(= ticket)
   $A \rightarrow E$: $K_{AS2}\{A\}$(= authenticator), $K_{S2}\{K_{AS2}\}$(= ticket)
   $E \rightarrow S_i$: $K_{AS2}\{A\}$(= authenticator), $K_{S2}\{K_{AS2}\}$(= ticket)

C. For instance we could solve this by using DNS.
   A certificate binds a public key to an entity (an identity like a person or organization). The binding occurs via a signature from an authority. Validation ensures the signature is present, and the entity presenting the certificate is who they say they are. The way you identify the peer is through DNS names. If DNS is compromised, or the hostname checks are omitted, then the system crumbles. So you need to trust *both* the certification authority *and* DNS. DNS does not provide authenticity assurances (or more correctly, clients don't use the security mechanisms), so you should consider DNS as untrusted input.

D. A possible attack could be to intercept A, $K_A\{K_{ASi}\}$ and$K_{ASi}\{A\}$. The attacker may try to hash all possible passwords and try to encrypt A with it. If this is equal to the $K_A\{K_{ASi}\}$ Alice sent back to the service, the we've found the correct hash for K_A and thus Alice's password.

Exercise 3

A. The purpose of diffie-hellman is to exchange a shared secret key. Alice and Bob want to have a shared public key. After one of the two has validated to others public key they know that only the other party has the shared key.
B. The protocol is as follows:
   $A \rightarrow B$: $A = g^a$
   $B \rightarrow A$: $B = g^b$
C. After they computed the shared key, they may encrypt a nonce with it and send it to each other.
D. $PK_{Alice} = A = g^a \bmod p = 19^{39} \bmod 101 = 71$
E. Bob will compute his shared key with Alice at the end. This computation is as follows: A^b

Exercise 4

A. $n = p * q = 11 * 19 = 209$
   Since p and q are prime, the euler function gives (p-1)(q-1).
   $\phi(n) = (11-1)(19-1) = 10 * 18 = 180$
B. To find the corresponding private key, we may use the extended euclidean algorithm. The starting pair will be (180, 17).

Pair	Remainder	Linear combination
(180, 17)	10 = 180 - 10 * 17	1 = **53** * 17 - 5 * 180 1 = 3 * 17 - 5 * (180 - 10 * 17)
(17, 10)	7 = 17 - 1 * 10	1 = 3 * 17 - 5 * 10 1 = 3 * (17 - 1 * 10) - 2 * 10
(10, 7)	3 = 10 - 1 * 7	1 = 3 * 7 - 2 * 10 1 = 1 * 7 - 2 * (10 - 1 * 7)
(7, 3)	1 = 7 - 2 * 3	1 = 1 * 7 - 2 * 3 1 = 0 * 3 + 1 * (7 - 2 * 3)
(3, 1)	0 = 3 - 3 * 1	1 = 0 * 3 + 1 * 1

   In the table above we see that private key d = 53
C. In RSA we know that $d * e = 1 \bmod \phi(n)$. This means that we may derive the public key from the private key in the same way as we may derive the private key from the public key.
   First, we compute $\phi(n) = (23 - 1)(19 - 1) = 22 * 18 = 396$

Pair	Remainder	Linear combination
(396, 317)	79 = 396 - 1 * 317	1 = **5** * 317 - 4 * 396 1 = 1 * 317 - 4 * (396 - 1 * 317)
(317, 79)	1 = 317 - 4 * 79	1 = 1 * 317 - 4 * 79 1 = 79 * 0 + 1 * (317 - 4 * 79)
(79, 1)	0 = 79 - 79 * 1	1 = 79 * 0 + 1 * 1

   Now, we see that the corresponding public key is 5.

Exercise 5

A. The passwords don’t need to be encrypted. In encryption there should be a way to decrypt the message back to the original message. However, passwords should be hashed which prevent an attacker from finding the original plaintext message from the hash.
B. Block cipher with electronic codebook mode (ECB)
C. Equal plaintext blocks give equal ciphertext blocks
D. I. The name of this technique is salting
   II. The technique adds a user-specific text to the passwords before hashing them.
   III. This technique ensures that users with equal password have different hashes stored in the database. If the password of one user has been discovered, this prevents that the attacker can find which other users have the same password.