Homework 5[1]

Question 1

Consider the toy key exchange protocol using an online trusted 3rd party (TTP) discussed in Lecture 9.1. Suppose Alice, Bob, and Carol are three users of this system (among many others) and each have a secret key with the TTP denoted k_a, k_b, k_c respectively. They wish to generate a group session key k_{ABC} that will be known to Alice, Bob, and Carol but unknown to an eavesdropper. How would you modify the protocol in the lecture to accomodate a group key exchange of this type? (note that all these protocols are insecure against active attacks)

1. Alice contacts the TTP. TTP generates a random k_{ABC} and sends to Alice

$$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow k_{ABC}, \quad \text{ticket}_2 \leftarrow k_{ABC}$$

Alice sends ticket_1 to Bob and ticket_2 to Carol.

2. Alice contacts the TTP. TTP generates random k_{ABC} and sends to Alice

$$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC}).$$

Alice sends ticket_1 to Bob and ticket_2 to Carol.

3. Alice contacts the TTP. TTP generates a random k_{ABC} and sends to Alice

$$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC})$$

Alice sends k_{ABC} to Bob and k_{ABC} to Carol.

4. Alice contacts the TTP. TTP generates a random k_{AB} and a random k_{AC}. It sends to Alice

$$E(k_a, k_{AB}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{AB}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{AC}).$$

Alice sends ticket_1 to Bob and ticket_2 to Carol.

Question 2

Let G be a finite cyclic group (e.g. $G = \mathbb{Z}_p^*$) with generator g. Suppose the Diffie-Hellman function $\text{DH}_g(g^x, g^y) = g^{xy}$ is difficult to compute in G. Which of the following functions is also difficult to compute: As usual, identify the f below for which the contra-positive holds: if $f(\cdot,\cdot)$ is easy to compute then so is $\text{DH}_g(\cdot,\cdot)$. If you can show that then it will follow that if DH_g is hard to compute in G then so must be f.

1. $f(g^x, g^y) = g^{xy+1}$

2. $f(g^x, g^y) = g^{x(y+1)}$

3. $f(g^x, g^y) = (g^2)^{x+y}$

4. $f(g^x, g^y) = (\sqrt{g})^{x+y}$

[1] https://class.coursera.org/crypto-012/

Question 3

Suppose we modify the Diffie-Hellman protocol so that Alice operates as usual, namely chooses a random a in $\{1,\ldots,p-1\}$ and sends to Bob $A \leftarrow g^a$. Bob, however, chooses a random b in $\{1,\ldots,p-1\}$ and sends to Alice $B \leftarrow g^{1/b}$. What shared secret can they generate and how would they do it?

1. secret $= g^{ab}$. Alice computes the secret as B^a and Bob computes A^b.

2. secret $= g^{a/b}$. Alice computes the secret as B^a and Bob computes $A^{1/b}$.

3. secret $= g^{a/b}$. Alice computes the secret as $B^{1/b}$ and Bob computes A^a.

4. secret $= g^{ab}$. Alice computes the secret as $B^{1/a}$ and Bob computes A^b.

Question 4

Consider the toy key exchange protocol using public key encryption described in Lecture 9.4. Suppose that when sending his reply $c \leftarrow E(pk,x)$ to Alice, Bob appends a MAC $t := S(x,c)$ to the ciphertext so that what is sent to Alice is the pair (c,t). Alice verifies the tag t and rejects the message from Bob if the tag does not verify. Will this additional step prevent the man in the middle attack described in the lecture?

1. it depends on what MAC system is used.

2. it depends on what public key encryption system is used.

3. yes

4. no

Question 5

The numbers 7 and 23 are relatively prime and therefore there must exist integers a and b such that $7a+23b=1$. Find such a pair of integers (a,b) with the smallest possible $a>0$. Given this pair, can you determine the inverse of 7 in $\mathbb{Z}_{23}$?

Question 6

Solve the equation $3x+2=7$ in $\mathbb{Z}_{19}$.

Question 7

How many elements are there in $\mathbb{Z}_{35}^*$?

Question 8

How much is 2^{10001} mod 11? (please do not use a calculator for this)

Question 9

While we are at it, how much is 2^{245} mod 35?
Hint: use Euler's theorem (you should not need a calculator)

Question 10

What is the order of 2 in $\mathbb{Z}_{35}^*$?

Question 11

Which of the following numbers is a generator of $\mathbb{Z}_{13}^*$?

1. 7, $\langle 7 \rangle = \{1,7,10,5,9,11,12,6,3,8,4,2\}$

2. 5, $\langle 5 \rangle = \{1,5,12,8\}$

3. 9, $\langle 9 \rangle = \{1,9,3\}$

4. 2, $\langle 2 \rangle = \{1,2,4,8,3,6,12,11,9,5,10,7\}$

5. 3, $\langle 3 \rangle = \{1,3,9\}$

Question 12

Solve the equation $x^2+4x+1=0$ in $\mathbb{Z}_{23}$. Use the method described in lecture 9.3 using the quadratic formula.

Question 13

What is the 11th root of 2 in $\mathbb{Z}_{19}$? (i.e. what is $2^{1/11} in \mathbb{Z}_{19}$)
Hint: observe that $11^{-1}=5$ in $\mathbb{Z}_{18}$.

Question 14

What is the discete log of 5 base 2 in $\mathbb{Z}_{13}$? (i.e. what is $\mathrm{Dlog}_2(5)$)
Recall that the powers of 2 in $\mathbb{Z}_{13}$ are

$$\langle 2 \rangle = \{1,2,4,8,3,6,12,11,9,5,10,7\}$$

Question 15

If p is a prime, how many generators are there in $\mathbb{Z}_p^*$?

1. $(p-1)/2$

2. $p-1$

3. $\varphi(p)$

4. $\varphi(p-1)$