CSE 350/550: Network Security, Quiz 2: TUE April 23, 2024 Name: ______________________, Roll No.: ____________

Instructions:

- There are 4 questions, each 8 marks, for a total of 32 marks. Total time available 30 minutes.
- Provide answers in the space provided only. You may do your rough work on a separate blank sheet.
- You may use a calculator, but nothing else. **Pl. keep your phones/laptops, books etc. away from you**.
- Do not use unfair means, else action will be taken. Do not use material such as books, notes, etc. or a computer, smart phone, etc. And do not share information with other students.

1. Alice & Bob plan to use ElGamal Cryptosystem to exchange messages confidentially. Bob sends to Alice a message, M1, that is encrypted using ElGamal Cryptosystem that itself uses Diffie-Hellman generated shared key, K. The underlying Diffie-Hellman parameters are: prime q = 19, and its primitive root a = 10. While Alice and Bob select private keys, XA & XB, unknown to an intruder, the public keys shared by Alice & Bob are YA = 3 and YB = 11. What is message, M1, given that the intruder has access to the computed cipher, C1 = 9? That is, what is M1, given: < q=19, root a=10, public keys YA=3, YB=11, cipher C1=9>. **Show all details.**

ALL CALC ARE MOD 19

Given $q=19$, $a=10$, $YA=3$, $YB=11$, $C1=9$

3

What is XA, given $YA=3=10^{XA} \Rightarrow XA=5$

OR What is XB, given $YB=11=10^{XB} \Rightarrow XB=6$

2

What is shared Diffie Hellman key, $K = YB^{XA} = 11^5 \pmod{19} = 7$

OR $K = YA^{XB} = 3^6 \pmod{19} = 7$

3

Given cipher $C1 = 9 = K * M1 = 7 * M1$, compute K^{-1}.

$K * K^{-1} = 1 \Rightarrow 7 * K^{-1} = 1 \Rightarrow K^{-1} = 11$

Given cipher $C1=9$, $K^{-1}=11$ $M1 = K^{-1} * C' = 11 * 9 = 4$

OR directly given cipher $C1 = 9 = K*M = 7*M \Rightarrow M1 = 4$

2. Device A wishes to send to device B a text, T1, and expects device B to reply with an acknowledgement, A1. Device B will accept text, T1, from A and then reply to it with an acknowledgement, A1, only if it is able to verify the origin & integrity of text sent by device A. Similarly, device A will accept the acknowledgement from device B only if it is able to (i) verify the origin and integrity of the reply, and (ii) the acknowledgement makes a reference to the earlier text, T1.
We assume devices A and B use an RSA-based public-key cryptosystem. They both have access to an RSA Certification Authority, CA, whose public key is known to both devices, A and B.

Write below:

2

a. What specific information should device A seek from Certification Authority, CA? And for what purpose?

A seeks from CA the Public-key certificate of B, so as obtain public-key of B, viz KPU-B

2

b. What specific information should device B seek from Certification Authority, CA? And for what purpose?

B seeks from CA the public key certificate of A, so as to obtain the public-key of A, viz KPU-A

Also write below:

2

c. what is the structure & content of the overall message that A sends to B, together with text T1, hash value, if any, encryption, if any, Nonce, if any.

A→B: E(KPR-A, [T1, Nonce1])

2

d. what is the structure & content of the overall message that B sends to A, together with ack, A1, hash value, if any, encryption, if any, Nonce, if any.

B→A: E(KPR-B, [A1, f(Nonce 1)])

(For an example from Kerberos, the structure & content of a communication from device AS to device C is specified as:
AS → C E(K_C, [K_B || ID_{TGS}]) || $Ticket_{TGS}$

3. Take a look at table below that describes a message together with the hash function/value. Here characters x_0, x_1, ... x_6 are message characters. The 8-bits of any character x_j are shown as: xj7, xj6, ..., xj0, where xj7 is the (EVEN) parity bit. That is
x07 + x06 + ... + x00 = 0; x17 + x16 + ... + x10 = 0; ..., x67 + x66 + ... + x60 = 0

A last character x_7 is added and forms part of the hash value. It is obtained by computing:
x70 + x60 + ... + x00 = 0; x71 + x61 + ... + x01 = 0; ...; x77 + x67 + ... + x07 = 0

		(parity) bit_7	bit_6	bit_5	bit_4	bit_3	bit_2	Bit_1	bit_0
x_0	I	x07	x06	x05	x04	x03	x02	x01	x00
x_1	O	x17	x16	x15	x14	x13	x12	x11	x10
x_2	u	x27	x26	x25	x24	x23	x22	x21	x20
x_3	1	x37	x36	x35	x34	x33	x32	x31	x30
x_4	2	x47	x46	x45	x44	x43	x42	x41	x40
x_5	0	x57	x56	x55	x54	x53	x52	x51	x50
x_6	0	x67	x66	x65	x64	x63	x62	x61	x60
(parity) x_7		x77	x76	x75	x74	x73	x72	x71	x70

To summarize, the sum of all bits in a given row is 0. And the sum of all bits in a given column is 0. The hash function consists of all the shaded bits from the table, viz. the bit_7 in each character, and the 8 bits in char_7. The rest is the original text.

I prepare a message consisting of 7 characters, "I O U 1 2 0 0", where the characters in the message are encoded as 8-bits including the parity bit. An 8 th character is added to complete the hash function/value. I now create a digital signature using the above hashing function, H(x), and RSA with my private key PR-BNJ.

2 a. Is it possible to replace the message to something else without this change being detected at the receiver's end? Yes in the above text
And why do you think so? At the very least, the ~~numbers~~ letters can be permuted, while the parity bits remain the same, e.g. 1200 → 2100.

2 b. Give one more example where it is possible to replace "IOU1200" without this change being detected at the receiver's end? IOU 2100 as also IOU 1233

1 c. Give one example where a change will in fact be detected at the receiver's end? IOU 1201

3 d. What change in the IOU note can be made by an intruder that will result in the largest value being owed by me, the sender? IOU 9974. If a student has written IOU 99xx give full marks.

4. A portion of the Kerberos v4 protocol is given below.

(1) $C \rightarrow AS$ $ID_c \| ID_{tgs} \| TS_1$

(2) $AS \rightarrow C$ $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) $C \rightarrow TGS$ $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) $TGS \rightarrow C$ $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$$

$$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$$

$$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) $C \rightarrow V$ $Ticket_v \| Authenticator_c$

(6) $V \rightarrow C$ $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$$

$$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$$

2 Pinpoint exactly which message, and specifically what content in the message, that allows:

A. The Authentication server (AS) to authenticate the client, C?
Message (2) AS → C the contents are encrypted using shared key K_c, without which client is unable to extract $Ticket_{tgs}$

2 B. Client, C, to authenticate itself to the Ticket-granting server, TGS
Message (3) C → TGS. Specifically "$Authenticator_c$" is encrypted by C using shared $K_{c,tgs}$ created / sent by AS

2 C. Client, C, to authenticate the Ticket-granting server, TGS?
From (3) $Ticket_{tgs}$, the TGS can obtain key $K_{c,tgs}$ that TGS uses to send message (4).

2 D. Client, C, to authenticate the sever, V?
As in C. above the server V obtains the key $K_{c,v}$ from $Ticket_V$ and uses that to reply message (6)