Your name: _____, Roll no.: _____, Your phone no. (optional): _____

CSE 350/550: Network Security, END-semester exam: May 7, 2024, 120 minutes, 120 marks

Instructions:

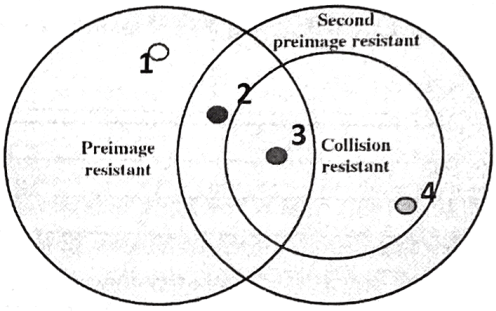
- The exam is in **two** parts: Part 1 consists of 6 questions that require short answers, each is for 5 marks ➔ 30 marks. Part 2 consists of 9 questions that require relatively long answers, each is of 10 marks ➔ 90 marks.
- This is a "closed-book" exam. All necessary information, including tables, etc. will be provided.
- Write your answers in the space provided. If necessary, use a separate sheet for rough work.
- Do not use unfair means. Action will be taken if you use unfair means. This includes using books, computer, phones, etc. or sharing information with other students. **You may use a calculator,** but nothing else.

Part 1: 6 questions that require short answers 5 marks each)

1. Hashing functions are classified based on whether the hash function satisfies one or more properties of "pre-image resistance", "second pre-image resistance" and "collision resistance" (see below). Clearly some hashing functions, such as '2', '3', and '4' given below, satisfy more than one property.
   Question: where could the hash function(s), '1', '2', '3', or '4' be used to implement (a) one-way passwords, (b) detect file tampering, or (c) digital signatures? To answer the question fill the table below.

1 mark each ⇒ 5 marks

Hashing function	One-way passwords	File integrity	Digital Signature
1	Yes/No	Yes/No	XXXXXXXX
2	Yes/No	Yes/No	Yes/No
3	Yes/No	Yes/No	Yes/No
4	XXXXXXXX	Yes/No	Yes/No



2. What makes the Diffie-Hellman scheme to compute a shared key so difficult to crack? That is, what is that fundamental property involving publicly known parameters viz. prime, q, its primitive root, a, and public keys, YA = a^XA, and YB = a^XB that makes it near-impossible for one to compute the shared key K or discover the private key XA or XB? Note all computations are mod q.

5 marks

If q is very very large prime no.:
Given $Y_A = a^{X_A}$, it is computationally infeasible to compute the discrete log of Y_A, viz. X_A. And similarly for X_B, given $Y_B = a^{X_B}$. This makes it impossible to computer shared key $K = a^{X_A X_B}$

3. Assume that multiple messages, M1, M2, and M3, are sent by Bob to Alice after encrypting them as C1, C2 and C3 using ElGamal cryptosystem and using the shared key, K, obtained using Diffie-Hellman cryptosystem. What is the perceived danger of using the same shared key, K to encrypt and send M1, M2, and M3?

5 marks

If 'somehow', an intruder is able to discover M1, then it can easily compute M2 and M3 by simply computing

$$M2 = \frac{M1 * C2}{C1} \quad \& \quad M3 = \frac{M1 * C3}{C1}$$

4. If protocol WPA2 over TLS/SSL is used in IEEE 802.11 WiFi networks, then what kind of message should AP send to client C so that client C can authenticate the AP. AND what information should the wireless client C possess so as to interpret this message and thereby authenticate the AP?

3 + 2

(i) AP should send a message to client C of the kind $E(PR\text{-}AP ; ID\text{-}AP)$ which client C can decrypt using Public key of AP. PR-AP = private key of AP

(ii) Client C should possess the CORRECT Public key of AP, whose ID is contained in the encrypted message

5. Consider the Kerberos protocol for user authentication. FOUR parties are involved: (1) client C, (2) AAA server, (3) TGS server, and (4) compute server V1. Now,
   i. What information should client C necessarily possess so that it can authenticate AAA, and be authenticated by AAA?

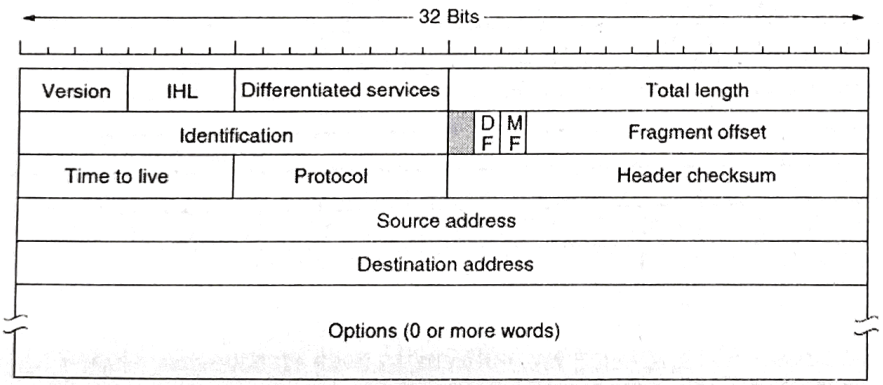
$2\frac{1}{2}$ + $2\frac{1}{2}$

(i) Client C should possess shared key K_C of the pre-established connection between C & AAA

(ii) Similarly, server V1 should possess the shared key K_{TGS} of the pre-established connection between TGS & server V1.

   ii. What information should server V1 necessarily possess so that it can authenticate TGS, and be authenticated by TGS?

6. Assume IIITD establishes a second campus in Noida, and connects the two LANs in Delhi and Noida by installing an IPSec "tunnel" between the corresponding routers in Delhi/Noida. Before an IP packet exits the egress router in Delhi LAN it is encrypted and encapsulated within a new IP packet.
   Question: Identify **4 fields** from the original IP header are NOT copied into the **IP header** of the **outer IP packet**? MORE Importantly explain why these fields should NOT be copied.
   FYI, the fields that make up an IPv4 header are shown below.



1 Total length
2 Time-to live
3 Header checksum
4 Source & Destination addresses

$\frac{1}{2}$ each $\Rightarrow$ 5 marks

Part 2: 9 questions that require somewhat longer answers (10 marks each)

7. An email addressed to user@cs.vu.nl is to be transferred from the sending mail server to the receiving mail server after undertaking several steps. Some of these are mentioned below. NOTE: these steps are NOT in the proper sequence. ALSO, some information is missing for each step. Other than completing the missing information for each step, state the sequence in which the 8 steps are undertaken. Supply your response below.

Total 10 marks

Incorrect sequence	Step to be undertaken	Fill in the missing information here	Correct sequence
1	Determine the IP address of the mail server using:	DNS server for cs.vu.nl	4
2	Access the DNS server relevant to:	cs.vu.nl (the ADMD)	2
3	Determine the URL of mail server from:	DNS server for cs.vu.nl	3
4	Transfer original headers and body together with:	hashvalue & signature	8
5	Compute the signature by encrypting the:	hashvalue	7
6	Compute the administrative mail domain from:	@mail address, ~~user~~ viz. cs.vu.nl	1
7	Compute the hash value from the given:	headers & body of email	5
8	Identify the key to be used to sign the:	DNS server for cs.vu.nl	6

3/4 marks each

½ mark each

8. A client C wishes to connect to a server V and use the services it offers. The connection can only be established after client C has authenticated the server V, and server V has authenticated the client C. In the present context, there exists no prior arrangement between the two. In other words, they do not have a shared key between them, and consequently, passwords cannot be sent to each other to authenticate each other. Under such circumstances how can they authenticate each other? That is:

   (a) What private or public information should client C and server V possess that will enable them to authenticate the other, or be authenticated by the other?

   Client C possesses:

   Public information: Public key of server V, PU-V
   Private information: Private key of client C, PR-C

   2 marks

   Server V possesses:

   Public information: Public key of client C, PU-C
   Private information: Private key of server V, PR-V

   2 marks

   (b) What is a sequence of messages that client C and server V send to each other so that client C and server V are able to authenticate each other? Hint: we may use a challenge-response paradigm, with nonce(s) as the challenge(s).

   Messages:

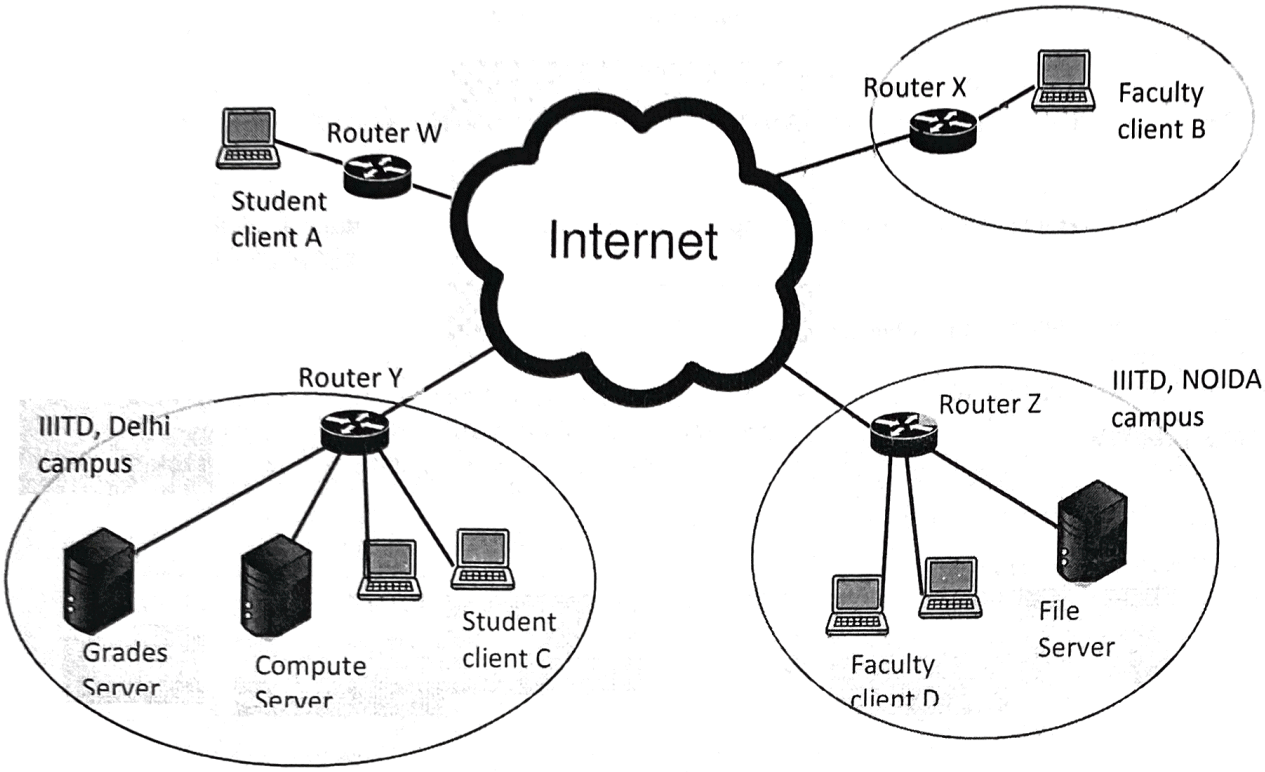
   1. C → V — M1: C || V || E(PU-V, Nonce1)
   2. V → C — M2: V || C || E(PU-C, f(Nonce1), Nonce2)
   3. C → V — M3: C || V || E(PU-V, f(Nonce2))
   4. V → C

   6 marks

   Alternatively:

   1. C → V — M1: C || V || E(PR-C, Nonce1)
   2. V → C — M2: V || C || E(PR-V, f(Nonce1), Nonce2)
   3. C → V — M3: C || V || E(PR-C, f(Nonce2))
   4. V → C

9. Consider establishing IPSEC 'Transport-mode' connections between clients and servers OR IPSEC 'Tunnel-mode' connections between routers so as to facilitate clients A, B, C, D to access the Grades server, Compute server & File server on the two campuses in Delhi or NOIDA.



(a) What kind of connection is required so that clients in either campus can access servers in local & remote campuses? Identify (i) the two end devices, and (ii) mode of IPSEC connection.

4 marks

Between routers Y & Z, "Tunnel-mode" connection

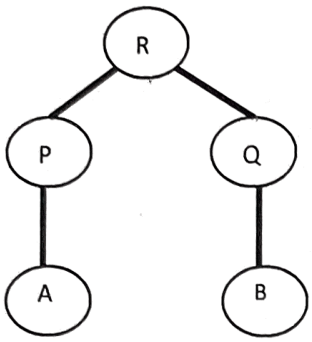
(b) What kind of none, one or more connections (possibly in different modes) need to be established so that faculty clients and student clients can access the three servers. NOTE: a student client may NOT access Grades server. Note, none, one or more connections may need to be established to facilitate or deny access. Use the table below to answer the question.

Client	Server	End devices & its	Mode of IPSEC connection	End devices & its	Mode of IPSEC connection
Student Client A	Compute/File server	Client A & compute server	Transport mode	client & file server	Transport mode
	Grades server				
Faculty Client B	Compute/File server	Routers X, Y	Tunnel mode	Routers X, Z	Tunnel-mode
	Grades server	Client B & Grades sever	Transport mode	—	—
Student Client C	Compute/File server	No additional connection	is required	once Tunnel-mode	
	Grades server				
Faculty Client D	Compute/File server	No additional connection is required	once Tunnel-mode conn.		
	Grades server	Client D & Grades server	Transport mode	—	—

1½ 2 1½ 2

Total 4 + 6 = 10

10. Consider the collection of entities A, B, P, Q and R that are either certification authorities or are users of certificates issued by such authorities. This is shown in figure below, where an edge describes the authority which originally signs the certificate. Since A does not possess the public-key of Q, PU-Q, it is unable to verify the certificate of B, CB-Q, issued and signed by Q.



(a) Other than the fact that entity A has B's certificate CB-Q signed by Q, what other information should entities A, B, P, Q and/or R possess before messages are exchanged between A, B, P, Q and R with the sole purpose of A verifying B's certificate CB-Q signed by Q and obtaining the public-key of B, PU-B?

4 marks

A: Public key of P, PU-P
B: —
P: Public key of R, PU-R
Q: —
R: Public key certificate of Q signed by R, CQ-R

(b) Now describe the steps that entities A, B, P, Q and/or R undertake to ensure that A has the public-key of B, viz. PU-B.

6 marks

1. A seeks from P, certificate CQ-P, signed by P
2. P seeks and obtains from R, certificate CQ-R, signed by R
3. P verifies CQ-R, extracts public key PU-Q, adds it to its directory
4. P creates certificate CQ-P signed by P, and delivers it to A
5. A verifies CQ-P, and extracts PU-Q, public key of Q; adds it to directory
6. A verifies CB-Q, using public key Q, PU-Q, extracts PU-B, public key of B.

11. Consider the field consisting of 4 bit numbers with defined operations "addition" and "multiplication", viz. **GF(2^4) = ({0000, 0001, ..., 1111}, +, *).** It is also assumed that the irreducible polynomial of degree 4 used to define arithmetic in **GF(2^4) is m(x,4) = $x^4 + x + 1$**. Then what is **4*6 + 1*C**, or **0100*0110 + 0001*1100** ?

$4 * 6 + 1 * C$

or $0100 * 0110 + 0001 * 1100$

or $x^2 * (x^2 + x) + 1 * (x^3 + x^2)$

$= x^4 + x^3 + x^3 + x^2$

$= x^4 + x^2$ — 4 marks upto here

$= x^2 + x + 1$ (reduced using $m(x) = x^4 + x + 1$)

or 0111 ↑ see

$x^4 + x + 1 \;)\; x^4 + x^2 \;(\; 1$

$x^4 + x + 1$

$x^2 + x + 1$

or $4 * 6 + 1 * C = 7$

another 6 marks

12. We propose to use ElGamal Cryptosystem for Bob to send 2 messages, M1 and M2, to Alice, but using Diffie-Hellman scheme to generate shared ONE-TIME SHARED KEYS whenever necessary. The specific Diffie-Hellman scheme uses prime q = 11, and its primitive root a = 2. Where/when necessary Alice draws random numbers from the sequence 8, 4, 3, etc., and Bob draws random numbers from the sequence 3, 9, 5, 2, etc.

A. List all steps to be undertaken by Alice and Bob in the proper order that together result in **first message M1 = 7** being sent by Bob and received by Alice, TOGETHER WITH NECESSARY CALCULATIONS OF Private/Public keys, Shared key, Cipher.

I. Alice selects PVT key $X_A = 8$; computes public key $Y_A = a^{X_A} = 2^8 = 3$; sends Y_A to Bob
II. Bob generates PVT key $X_{B1} = 3$; computes public key $Y_{B1} = a^{X_{B1}} = 2^3 = 8$
III. Bob uses Alice's public key $Y_A = 3$ to compute shared one time key $K_1 = Y_A^{X_{B1}} = 3^3 = 5$
IV. Bob encrypts message $M_1 = 7$ as $C_1 = M_1 * K_1 = 7 * 5 = 2$
V. Bob sends public key Y_{B1} & $C_1 = 2$ to Alice
VI. Alice computes shared one-time key $K_1 = Y_B^{X_A} = 8^5 = 5$
VII. Alice computes K_1^{-1} as $K_1^{-1} * K_1 = 1$ or $K_1^{-1} * 5 = 1 \Rightarrow K_1^{-1} = 9$
VIII. Alice computes $M_1 = K_1^{-1} * C_1 = 9 * 2 = 7$
IX.

6 marks

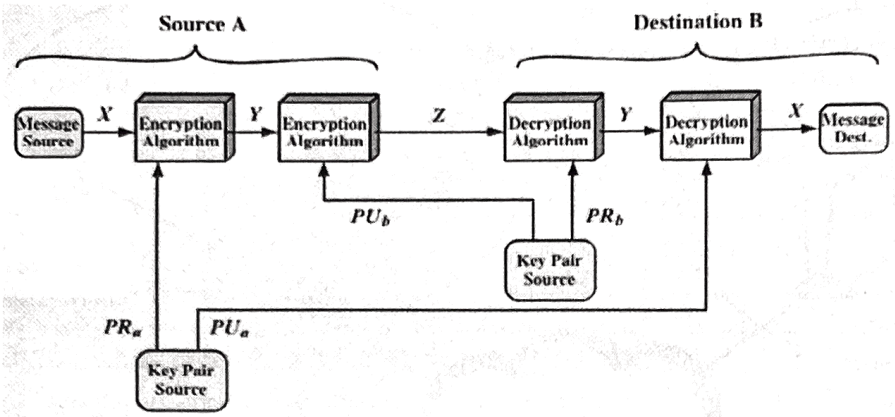
B. List all steps to be undertaken by Alice and Bob that together result in second message **M2 = 8** being sent by Bob and received by Alice, TOGETHER WITH NECESSARY CALCULATIONS OF Private/Public keys, Shared key, Cipher.

X. Bob generates new PVT key $X_{B2} = 9$; computes $Y_{B2} = 6$
XI. Bob computes shared key $K_2 = Y_A^{X_{B2}} = 3^9 = 4$
XII. Bob computes cipher $C_2 = M_2 * K_2 = 8 * 4 = 10$; sends $Y_{B2} = 6$ & $C_2 = 10$ to Alice
XIII. Alice computes new shared one-time key $K_2 = Y_{B2}^{X_A} = 6^8 = 4$ & computes $K_2^{-1} = 3$
XIV. Alice computes $M_2 = K_2^{-1} * C_2 = 3 \times 10^0 = 8$
XV.
XVI.

4 marks

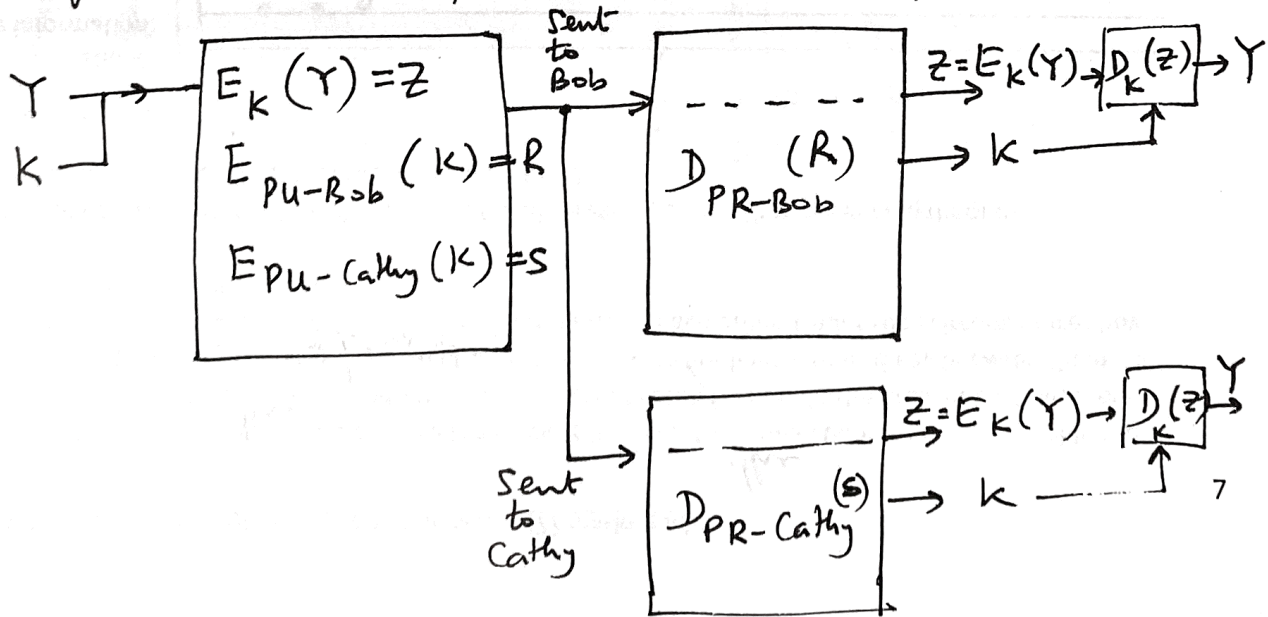
Total 10 marks

13. One way for Alice to send a message M to Bob is to (a) prepare the message M, (b) sign it using her private RSA key, PR-A, (c) encrypt the concatenated M || signed(H(M)) using Bob's public RSA key, PU-B, and (d) send the resultant to Bob. This is illustrated below.



But, presently Alice wishes to also copy the message to Bob and her friend Cathy, simultaneously, without having to encrypt the concatenated M ll signed(H(M)) twice. That being so, how can the above step (c) be changed so that both Bob and Cathy are able to decrypt the message but no one else can? The answer is best illustrated by YOU by adding a diagram.

2 marks each ⇒ total 10 marks

1. The message X together with its signature ~~is~~, YIZ Y is encrypted using a symmetric ~~key~~ cryptosystem that uses ~~shared~~ key k.
2. The key k is sent to both Bob & Cathy, but suitably encrypting it with Bob's public-key (from RSA), Pu-Bob and ~~*~~ Cathy's RSA public key, PU-Cathy.
3. Bob & Cathy can respectively decipher the key using their own RSA private keys, PR-Bob & PR-Cathy, and decrypt the message Y that was encrypted using symmetric crypto-system that uses key k.
4. The advantage is that the message Y is NOT encrypted twice. Only the key k is encrypted twice.
5. 

14. 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 such that:

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	x07	x06	x05	x04	x03	x02	x01	x00
x_1	x17	x16	x15	x14	x13	x12	x11	x10
x_2	x27	x26	x25	x24	x23	x22	x21	x20
x_3	x37	x36	x35	x34	x33	x32	x31	x30
x_4	x47	x46	x45	x44	x43	x42	x41	x40
x_5	x57	x56	x55	x54	x53	x52	x51	x50
x_6	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 now prepare a message consisting of 7 characters, "I O U 2 1 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 RSA-based digital signature using the above hashing function, H(x), with my private key PR-BNJ.

4 marks

a. Give two examples where it is possible to replace "IOU2100" without this change being detected at the receiver's end? IOU 1200 IOU 2133

2 marks

b. Give one example where a change will in fact be detected at the receiver's end?
IOU 2011

4 marks

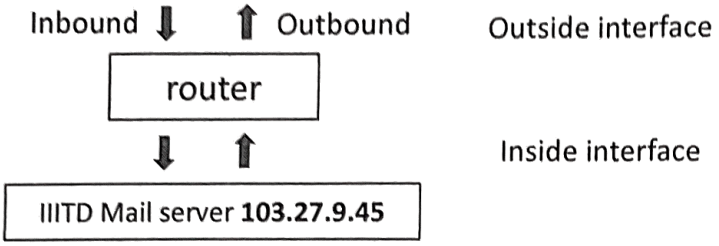
c. What change in the IOU note can be made by an intruder that will result in the largest value being owed by me, the sender?
IOU 8865
Explain as to why this change will not be detected:
The parity bits concerning the integers 2100 & 8655 are unchanged.

I		. . . .
O		. . . .
U		. . . .
8	1	1 0 0 0
8	1	1 0 0 0
6	0	0 1 1 0
5	0	0 1 0 1
	0	0 0 1 1

I		. . . .
O		. . . .
U		. . . .
2	1	0 0 1 0
1	1	0 0 0 1
0	0	0 0 0 0
0	0	0 0 0 0
	0	0 0 1 1

The total 10 marks

15. Consider writing rules for a router/firewall to filter (viz. 'permit' or 'deny') inbound or outbound **EMAIL related traffic** into or from IIITD LAN network on its "**Outside interface**" (see Figure below). The range of IP addresses visible outside IIITD are **103.27.8.0/22**. IIITD hosts its email server at IP address **103.27.9.45**. It listens to incoming emails on its **port 25**.



a. The following two entries are made in the table corresponding to **OUTBOUND** Traffic.

OUTBOUND traffic							
	Permit/Deny	Protocol	Source IP addr	Source port	Dest IP addr	Dest Port	Interface
1	Permit	tcp	103.27.9.45	any	any	25	**Outside I/F**
2	Deny	tcp	103.27.8.0/22	any	any	25	**Outside I/F**

How do you interpret these entries in the table for **OUTBOUND** traffic on **Outside** interface: that is what is it that is allowed, and what is it that denied?

Above (i) permits outbound packets from IIITD mail server (103.27.9.45) to any mail server on port 25
(ii) denies outbound packets from any other server in IIITD to mail servers on port 25 elsewhere

2+2 marks

b. The following entries are made in the table corresponding to **INBOUND** Traffic.

INBOUND traffic							
	Permit/Deny	Protocol	Source IP addr	Source port	Dest IP addr	Dest Port	Interface
1	Permit	tcp	any	25	103.27.9.45	any	**Outside I/F**
2	Deny	tcp	any	25	103.27.8.0/22	any	**Outside I/F**

How do you interpret these entries in table for **INBOUND** traffic on **Outside** interface: that is what is it that is allowed, and what is it that denied?

Above (i) permits inbound packets received in response from any mailserve elsewhere to packets sent by IIITD mail server in Q. above
(ii) denies inbound packets ~~to any~~ from any mailserver elsewhere to any server in IIITD

1½ + 1½ marks

c. The following entries are **ADDITIONALLY** made in the table corresponding to **INBOUND** Traffic.

INBOUND traffic							
	Permit/Deny	Protocol	Source IP addr	Source port	Dest IP addr	Dest Port	Interface
1	Permit	tcp	any	any	103.27.9.45	25	Outside I/F
2	Deny	tcp	any	any	103.27.8.0/22	25	Outside I/F

How do you interpret these **ADDITIONAL** entries in table for **INBOUND** traffic on **Outside** interface: that is what is it that is allowed, and what is it that denied?

Above (i) permits inbound packets from any server elsewhere to mailserver in IIITD (103.27.9.45) on port 25
(ii) denies inbound packets from any server elsewhere to any other server in IIITD on port 25.

½ + ½ marks

Total marks = 10