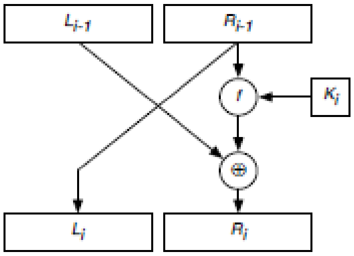
Sardar Patel Institute of Technology

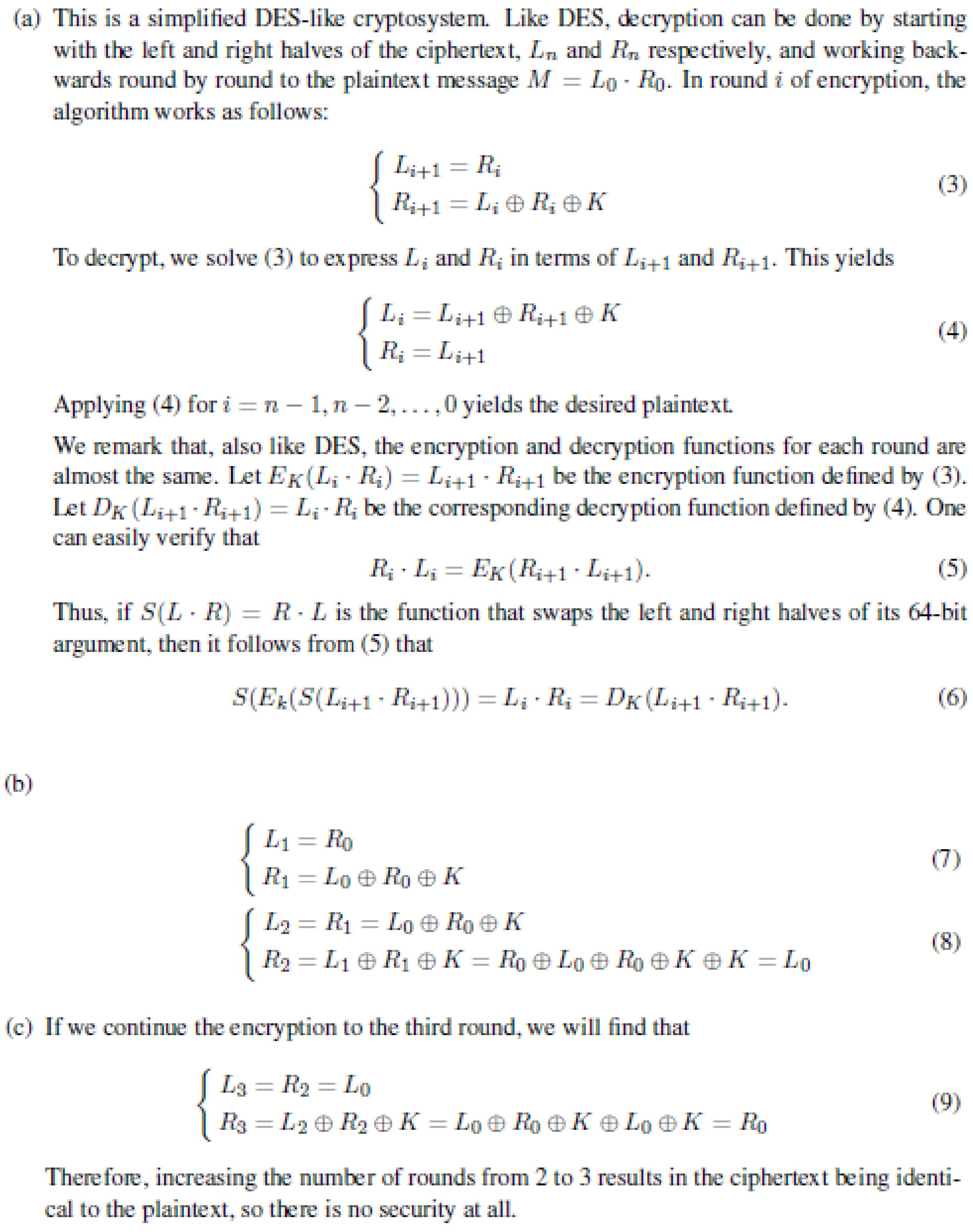
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058, India
(Autonomous College Affiliated to University of Mumbai)
TE (COMP+IT), Sem V, End Semester Exam
Sub: Cryptography and System Security, Code: CS307A
21st Dec 2021

Max. Marks: 60 **Duration: 2 Hrs**

Instruction: *Keep your answers clear and concise, and state all of your assumptions carefully. Answer **ALL** questions*

Qn		M(CO)
Q.1	Answer any **Five** from following	15(1,2,3)
a	Let us say that you are acting as an eavesdropper and observing an encrypted conversation between Sun and Moon. You notice that the prefixes of many of the cipher texts agree for several hundred bytes. In addition, these identical prefixes are always a multiple of 16 bytes long. However, you never observe two identical chunks of cipher text of any significant length following the identical prefixes. Conjecture what cipher is being used, what mode of operation is being used, and what Sun and Moon are doing wrong.	(3)
	Solution: The answer we had in mind was AES (or DES) under CBC mode, (incorrectly) using the same IV for every message. Full credit will be given for an answer such as AES or DES in ECB mode, with some explanation (e.g., all messages have long, common headers.)	(3)
b	In its next chip, Intel finds a way to make the stack non-executable. Does this solve the problem of buffer-overflow attacks? Explain briefly. Solution: No. It's still possible to maliciously modify the return address and parameters on the stack, which could cause undesired behavior.	(3)
c	Why is it required that the private and public keys in RSA are relatively-prime to -Φ(n)? Suppose Φ(n) = 18, choose two legal values for public and private keys (don't forget to include n). Solution: If a key is not relatively-prime, then it has no modular inverse, and we cannot generate a key pair. Plus, the substitution is not one-to-one for these numbers, so we do not get a proper encryption, either. If Φ(n) is 18, then we can choose d = 5 as it is relatively-prime to 18. A multiplicative inverse of d mod18 is e = 11. Since n = pq and Φ(n) = (p − 1)(q − 1), then n can equal (3 + 1)(6 + 1) = 28 or (2 + 1)(9 + 1) = 30 or (1 + 1)(18 + 1) = 38. Only the last is the product of two primes, so a private key is {5,38} and a public key is {11,38}.	(3)
d	Explain briefly similarities and differences between cryptographic hash functions and message authentication codes (MAC's). Solution: Both take as argument an arbitrarily long message and produce a short (typically 160 or 256 bits) result. The MAC takes additionally a secret key as argument. Both are used to ensure integrity, i.e. that a message has not been tampered with. A MAC additionally provides authentication, i.e. evidence about who the sender is. Hash functions have many additional uses in cryptography.	(3)

e	Assume that system administrator in SPIT tries to setup email facility and he tries to use the simple mail transfer protocol (SMTP). Now this protocol is severely limited in terms of security. Hence what are the three main security threats, system administrator should visualize as a part of system security? Justify identified threats.. Answer: 1. Authenticity-related threats: The receiver may not know if the email is coming from a legitimate source. 2. Integrity-related threats: The receiver may not know if the message was modified in transit. 3. Confidentiality-related threats: The message is subject to unauthorized disclosure of sensitive information. 4. Non-repudiation threat: The sender may deny sending the message. 5. Availability-related threats: Could prevent end users from being able to send or receive email.	
f	Given an encryption function f(x), what kinds of trials can you do in order to check whether or not it achieves avalanche effect? Give example and explain. Also how S-box and P-box contributes to block cipher to achieve avalanche effect. Solution: We can try two strings that are different in only one element, for example: f(ABCD) and f(ACCD). If at least 50% of the resulting cipher text of one of the inputs is different from that of the other, then we can conclude that it achieves diffusion, and vice versa. • S-box: contributes to confusion, as it substitutes elements for others, this way making the relationship between the plain and cipher text weaker. • P-box: contributes to diffusion, as the permutation steps are essential in order to reach a totally different cipher text if only one element of the plain text is changed.	
g	Draw a schematic view SSL protocols with suitable notaions. Identify the name of protocol for the following given functionality: 1) Establishes the security capability 2) Connection failure and illegal parameters 3) Provides confidentiality and message integrity	
h	Name mail access protocols and Compare them	
	.	
Q.2		15(2,4)
a	Recall that the heart of DES is a round of the form:  Consider a simplified DES-like cryptosystem consisting of n such rounds, where the function f is defined by $f_K(X) = K \oplus X$. Here we assume that the key K is 32-bits long and that the same key is used at each round, that is, Ki = K for each round i. This system is used to encrypt a 64-bit message M as follows: L0 is the leftmost 32-bits of M and R_0 is the rightmost 32-bits of M. The ciphertext $E_K(M)$ is Ln . Rn. a) Describe how to decrypt messages encrypted with E_K.	8

	b) Express L_1, R_1, L_2, and R_2 in terms of L_0, R_0, and K. c) If we increase number of rounds then it will increase security or decrease security? Justify your answer by showing proof	
	Solution a) This is a simplified DES-like cryptosystem. Like DES, decryption can be done by starting with the left and right halves of the ciphertext, Ln and Rn respectively, and working backwards round by round to the plaintext message M = L0 _ R0. In round i of encryption, the algorithm works as follows  (a) This is a simplified DES-like cryptosystem. Like DES, decryption can be done by starting with the left and right halves of the ciphertext, L_n and R_n respectively, and working backwards round by round to the plaintext message $M = L_0 \cdot R_0$. In round i of encryption, the algorithm works as follows: $\begin{cases} L_{i+1} = R_i \\ R_{i+1} = L_i \oplus R_i \oplus K \end{cases} \qquad (3)$ To decrypt, we solve (3) to express L_i and R_i in terms of L_{i+1} and R_{i+1}. This yields $\begin{cases} L_i = L_{i+1} \oplus R_{i+1} \oplus K \\ R_i = L_{i+1} \end{cases} \qquad (4)$ Applying (4) for $i = n-1, n-2, \ldots, 0$ yields the desired plaintext. We remark that, also like DES, the encryption and decryption functions for each round are almost the same. Let $E_K(L_i \cdot R_i) = L_{i+1} \cdot R_{i+1}$ be the encryption function defined by (3). Let $D_K(L_{i+1} \cdot R_{i+1}) = L_i \cdot R_i$ be the corresponding decryption function defined by (4). One can easily verify that $R_i \cdot L_i = E_K(R_{i+1} \cdot L_{i+1}). \qquad (5)$ Thus, if $S(L \cdot R) = R \cdot L$ is the function that swaps the left and right halves of its 64-bit argument, then it follows from (5) that $S(E_k(S(L_{i+1} \cdot R_{i+1}))) = L_i \cdot R_i = D_K(L_{i+1} \cdot R_{i+1}). \qquad (6)$ (b) $\begin{cases} L_1 = R_0 \\ R_1 = L_0 \oplus R_0 \oplus K \end{cases} \qquad (7)$ $\begin{cases} L_2 = R_1 = L_0 \oplus R_0 \oplus K \\ R_2 = L_1 \oplus R_1 \oplus K = R_0 \oplus L_0 \oplus R_0 \oplus K \oplus K = L_0 \end{cases} \qquad (8)$ (c) If we continue the encryption to the third round, we will find that $\begin{cases} L_3 = R_2 = L_0 \\ R_3 = L_2 \oplus R_2 \oplus K = L_0 \oplus R_0 \oplus K \oplus L_0 \oplus K = R_0 \end{cases} \qquad (9)$ Therefore, increasing the number of rounds from 2 to 3 results in the ciphertext being identical to the plaintext, so there is no security at all.	
b	Consider the scenario where Sun receives a contract *m* from Moon, together with	7

	Moon’s signature *s* on this document. Sun can then show to anyone that Moon has signed *m*. However this property is unsuitable for some applications, where Moon’s commitment to *m* may be sensitive. For such situations, Neptune suggested *undeniable signatures*. An *undeniable signature* can only be verified with cooperation from the signer. To verify signature *s*, the verifier Venus engages in a protocol with Moon. Presume that Moon agrees to interact with Venus. So while running this verification protocol which equality does Venus then check to verify the signature? Draw suitable diagram and explain. Indicate clearly your assumption and parameters that you consider. (Hint: a cyclic group G of prime order q with generator g and a hash function H with hash values in G. Each signer chooses a private key x € Z^*_q and computes the public key $X = g^x$. The signature on m is $s = (H(m))^x)$	
	Solution Venus chooses random integers a and b, both smaller than q, and computes the challenge $c = s^aX^b$, which is sent to the signer Moon. Moon responds by sending back $r =c^{xl}$, where x0 is the inverse of x in Z € q, i.e. xx’ =1(mod q). For a correctly signed message we have that $r = c^{x'} = (s^aX^b)^{x'} = (H(m)^{xa}g^{xb})^{x'} = H(m)^a g^b,$ where the last equality makes use of the fact that $xx' = 1(\bmod q)$. where the last equality makes use of the fact that xx’ = 1(mod q). So, Venus checks that $r = H(m)^a g^b$	
Q.3		15(2,3)
a	Tom and Jerry proposed the following protocol in which A and B use a MAC algorithm, and a long-term shared key K_{AB} for this MAC, to agree on a session key K_S: 1: A→B : A;N_A 2: B→A : N_B; MAC $K_{AB}(N_A \Vert N_B \Vert B) \oplus K_S$ a) Show how session key will be computed by A? b) Explain for both A and B why they believe after a run that the session key K_S is fresh, i.e. that they are not subject to a replay attack which establishes some old session key. c) Crackle simplifies the protocol as follows where he believes that since B chooses a new random key K_S in message 2, his nonce N_B is not necessary and he exchanges following protocol 1: A →B : A;N_A 2: B→A : MAC$K_{AB}(N_A \Vert B) \oplus K_S$ If adversary gets hold of above simplified protocol then what he can do? Will B able to maintain communication with A or not? Justify your answer. d) Do you think that there should be KDC or Third party required to improve the trust among A and B communication in a)? Yes or No? Justify	8
	Solution:	

	(a) He concatenates his own nonce, the received nonce and B:s identity and computes the MAC of this. He then takes the xor of this with the second part of the received message and this is the session key. (b) A believes that the key is fresh, since its computation involves her own freshly chosen nonce. B knows that it is fresh, since he chose it himself before sending message 2. (c) If the adversary gets hold of the session key for a session where he has recorded the protocol run, then he can xor the key and the second part of the recorded message 2. This will give him $\text{MACK}_{AB}(N_A \Vert B)$ for the nonce that A chose. He can then, whenever he pleases, start a new run, pretending to be A and using the same nonce NA. If B does not check the reuse of the nonce (which is commonly omitted), he will proceed with the protocol and the adversary can use his saved MAC value to compute the session key. (d) One reason is that it is a matter of trust to allow someone to choose a key which you will use. Thus, a trusted third party, who by definition is trusted, is a better choice than an arbitrary user you need to communicate securely with.	
b	Gromit wants to send a Whatsapp message to Wallace securely, over an insecure satellite network. Gromit's device has a RSA public key K_G and matching private key V_G; likewise, Wallace's device has K_W and V_W. Let's design a cryptographic protocol for doing this, assuming both know each other's public keys. Here is what Gromit's device will do to send the text message m: 1) Gromit's device randomly picks a new AES session key k and computes c’ = RSA-Encrypt (K_W; k), c’= AES-CBC-Encrypt (k;m), and t = RSA-Sign(V_G; (c; c’)). 2) Gromit's device sends (c; c; t) to Wallace's device. And here is what Wallace's device will do, upon receiving (c; c’ ; t): 1) Wallace's device checks that t is a valid RSA signature on (c; c’) under public key K_G. If not, abort. 2) Wallace's device computes k’ = RSA-DecryptV_W; c) and m’ = AES-CBC-Decrypt (k’; c’). 3) Wallace's device informs Bob that Gromit has sent message m’. a) Does this protocol ensure the confidentiality of Gromit's messages? Why or why not? b) Does this protocol ensure authentication and data integrity for every text message Wallace receives? Why or why not? c) Suppose that Wallace is Gromit's financial advisor. Wallace hooks up the output of this protocol to an automatic financial trading service, so if Gromit sends a Whatsapp message ‘Sell 1000 shares of L&T’ using the above protocol, then this trade will be immediately and automatically executed from Gromit's account. From security point of view is this a good idea or not? At least give one proper reason that justifies your suggestion. d) Explain how an adversary can recover the secret key when the signer reuses the same random number r for two different messages. State your assumptions also clearly (*Hint:* This is a digital signature scheme, so a message needs to be sent along with its signature)	7

	a) Yes. Since AES-CBC-Encrypt is secure, no one can recover m from c’ without knowledge of k. Also, since RSA-Encrypt is secure, only someone who knows K_B—namely, Gromit—can recover k. b) Does this protocol ensure authentication and data integrity for every text message W receives? Why or why not? Yes. Since RSA-Sign is secure, if (c; c’) passes step 1, then only someone who knew v_W—namely, Wallace— could have sent (c; c’). Now (c; c’) uniquely determines m, the message that Wallace wanted to send. Conclusion: If Grommit accepts m in step 3, then G sent m. c) Suppose that W is G's stockbroker. W hooks up the output of this protocol to an automatic stock trading service, so if G sends a text message “Sell 100 shares of L&T” using the above protocol, then this trade will be immediately and automatically executed from G's account. Suggest one reason why this might be a bad idea from a security point of view. No protection against replays. An active attacker could replay a valid ciphertext from G 10 times, causing 1000x10 shares to be sold—even though Gonly wanted 100 sold. Denial-of-service. An active attacker could prevent G’s ciphertext from reaching W. Since G doesn’t receive any acknowledgement, he will think her trade was executed, when it actually wasn’t. If G’s cellphone is lost or stolen, then its new owner can cause trades to be executed from Alice’s account without G’s authorization. d) Explain how an adversary can recover the secret key (i.e., x) when the signer reuses the same random number r for two different messages. State your assumptions also clearly. (Hint: This is a digital signature scheme, so a message needs to be sent along with its signature) Solution d) Consider two signatures [k, c1] and [k, c2] for messages m1 and m2 respectively. c1 - c2 = (m1 – x k - m2 + x k) r $^{-1}$ mod p - 1 (c1 - c2) r = (m1 - m2) mod p -1 Assume (c1 - c2) has an inverse in mod p - 1. r = (c1 - c2)$^{-1}$ (m1 - m2) mod p -1 Once you learn r, it is easy to find x: x = (m1 - c1 r) k^{-1} mod p - 1.	
Q.4		15(4)
a	What is stateful and stateless firewall? Suppose a host-based firewall on a server keeps state for existing TCP connections—i.e., it tracks the state of TCP handshakes and only allow non-handshake packets on established connections. It must create a “SYN-received/SYN-ACK sent” queue until it sees a responding “ACK.” Since the firewall queue is finite, it can be overwhelmed by a SYN-flood attack in which an attacker node sends many requests (SYN packets) under spoofed IP addresses, to cause the firewall to run out of queue space. i) What will happen if, when the firewall runs out of queue space, it blocks further SYN packets? ii) What will happen if, when the firewall runs out of queue space, it stops enforcing the restriction on non-handshake packets? iii) Explain why an ACK time-out strategy will not work to solve this problem. Answer:	8

	A stateless firewall does not keep information about existing connections, TCP sequence numbers, and other information. It analyzes packets independently, not as part of the packet sequence i) In the first case, the firewall will cause a denial-of-service attack on the server by dropping any further connection requests ii) The firewall will loose the ability to enforce the restriction of not accepting non-handshake packets on non-established connections, since it will no longer have knowledge of the set of established connection. iii) An ACK time-out strategy will not work against a large attack. An attacker can generate enough SYN packet to make sure the buffer is filled up before the first ACK time-out takes place.	
b	Let us say that global corporation establishes gateways GW1 and GW2 at different branches. They enable machines in different branches to communicate securely over the Internet by implementing IPSec at the gateways only. That means that when a machine A inside the first network sends an IP packet to a machine B in the second network, the gateway GW1 intercepts the IP packet in transit and encapsulates it into an IPSec packet. At the other end, GW2 recovers the original IP packet to be routed in the second network to machine B. Which of the IPSec modes and protocols should be used if it was desired that no Internet eavesdroppers learn about the identities A and B of the communicating parties. Draw figure with suitable notations and explain, Solution: If the identities of the communicating parties must be kept secret (protection against traffic analysis), then tunnel mode with encryption (ESP) should be used. In this case, the original IP packet header (which identifies source and destination machines) is encrypted and sent as payload. The new IP header will only show GW1 and GW2 as the source/destination pair	7