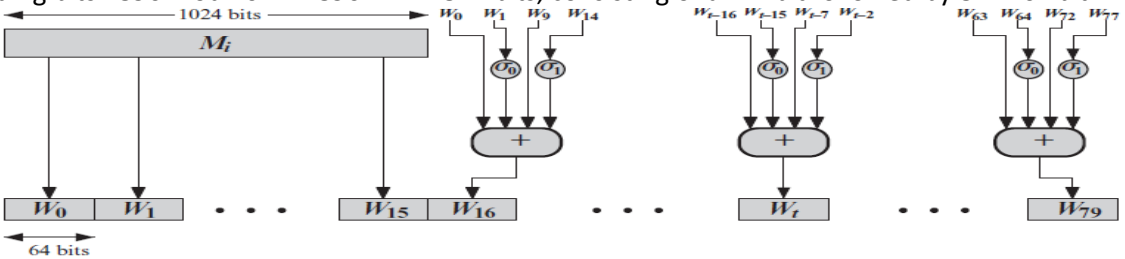
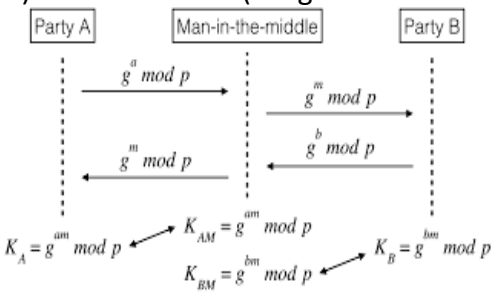
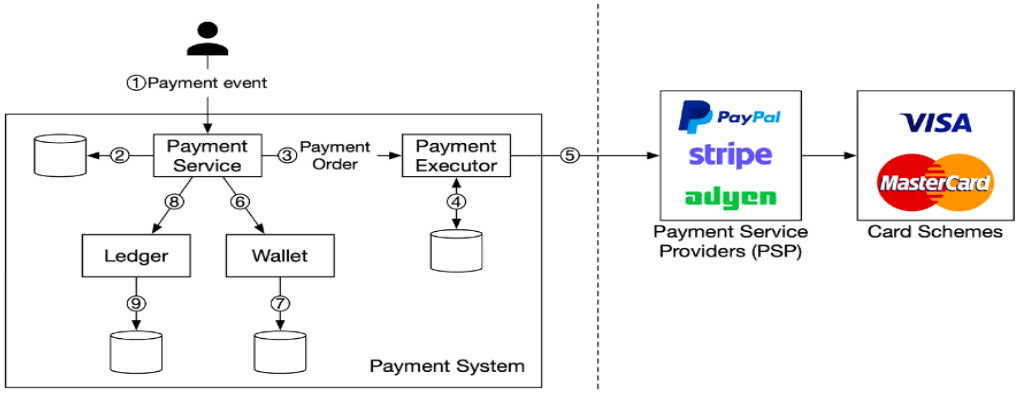
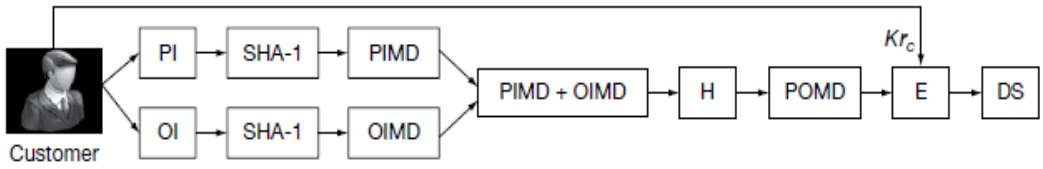
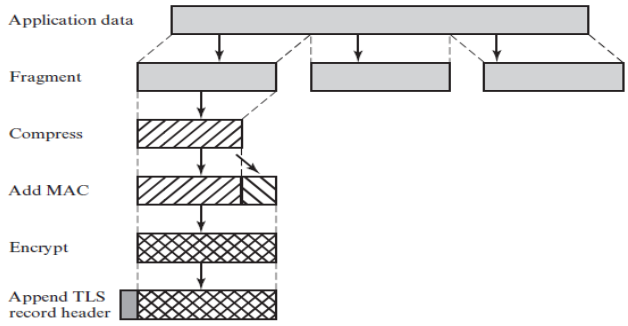
	Final Assessment Test – Winter 2023-24 Semester - May 2024	
Vellore Institute of Technology (Deemed to be University under section 3 of the UGC Act, 1956)	Course code : BCSE309L	Slot: E2 + TE2
	Course Title : Cryptography and Network Security	Time: **Three Hours**
	Course Mode **: CBL**	Max. Marks: **100**
Emp Id: 20131	Faculty Name : R Mariappan	School: SCOPE

ANSWER KEY

Sl No	Question Text	Marks
1 A)	A child has some fruits in a box. If the fruits are grouped in 7's, there will be 5 left over; If they are grouped in 11's, there will be 6 left over; If they are grouped in 13's , 8 will be left over; Find the least number of fruits in the box.	
Ans	Let x be the least number of fruits in the box, then x≡5(mod7); x≡6(mod11); x≡8(mod13); We can use Chinese remainder theorem to find x a1=5; a2=6; a3=8; m1=7; m2=11; m3=13; M=m1×m2×m3=1001 M1=M/m1=143 M2=M/m2=91; M3= M/m3=77 M1y1≡1(mod7)⟹143y1≡1(mod7)⟹3y1≡1(mod7) ===> y1≡5(mod7) M2y2≡1(mod m2)⟹91y2≡1(mod11)⟹3y2≡1(mod11) ⟹y2≡4(mod11) M3y3≡1(modm3)⟹77y3≡1(mod13)⟹12y3≡1(mod13) ⟹y3≡12(mod13) The solutions to this system are those x such that x≡M1y1a1+M2y2a2+M3y3a3(mod m) ⟹x≡143(5)(5)+91(4)(6)+77(12)(8)(mod1001) ⟹x≡13151(mod1001) ⟹x≡138(mod1001) This shows that the least number of fruits in the box is 138.	2 2 1
1.B)	Find last 2 digits of 9^{100}.	
Ans	**Last 2 digits: 0 1** Applying Euler's / Fermat's theorem : 1 mark Last 1 digit (1) (correct): 2 marks; Last 2 digits (01)- correct: 4 marks	 1 4
2 A)	Use extended Euclidean algorithm to find the GCD and MMI of (42823, 6409) and its linear combination.	
Ans	GCD = 17 MMI = Not exist as they are not co-prime 42823 * x + 6409 * y = 17 has a solution of (x,y) = (-22,147)	1 1 3
B)	B)Find 3^{64} mod 67 using Fermat's theorem	
Ans	Applying Fermat's little theorm , $a^{p-1} \equiv 1 \bmod p$ 3^{64} mod 67 = 15 (with all steps)	1 4
3	In DES, given that K= 133457799BBCDFF1, generate subkeys K1,K2,K3	
Ans	DES Key generation algorithm (diagram) K1 = 000110 110000 001011 101111 111111 000111 000001 110010 (C0 & D0 only: 1mark) K2 = 011110 011010 111011 011001 110110 111100 100111 100101 (C1 & D1 only : 1mark) K3= 010101 011111 110010 001010 010000 101100 111110 011001 (C2 & D2 only : 1mark)	2 3 3 2

4	In AES, M={0F0E0D0C0B0A09080706050403020100} and K={02020202020202020202020202020202, Show initial and final State matrix after MixColumns	
Ans	Initial State Matrix 0F 0B 07 03 (1 mark) Final State Matrix 0D 09 05 01 0E 0A 06 02 08 0C 00 04 0D 09 05 01 0F 0B 07 03 0C 08 04 00 0A 0E 02 06 **Note: If only 1 , 2 columns are calculated correctly, then '5', '10' marks may be awarded.**	Init state mat:1M 1 col: 5M 2 col:10M
5. A)	Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 71 and its primitive root=7 a. If Bob has public key YB = 4 ,what is Bob's pvt key XB? b. If Alice has public key YA = 51 , what is the shared key K with Bob.	
Ans	a. Xb =12 b. Xa=5; K= 30	2 2
B)	B)In Elgamal cryptosystem, global prime p =107, generator g=2. Alice chooses private key Xa=67 and Bob's unique random integer k=45. Encrypt the message ='A' (ASCII:65)	
Ans	Alice Public Key Ya=2^67 ≡ 94 (mod 107). Writing all 3 formulas C1= 2^{45} (mod 107)= 28 C2= 94^{45} (65) (mod 107) = 5(65) (mod 107) = 4	2 2 2
6.	Consider the elliptic curve $y^2 = (x^3 + 9x + 17) \bmod 23$. which belongs to $E_{23}(9, 17)$. Find the discrete logarithm value 'n' for the equation Q = nP, where Q = (4, 5) and P = (16, 5).	
Ans	The point addition and point Doubling operations are used to perform brute-force method as follows. Formulas for slope 'm', x3, y3 P = (16, 5); 2P = P + P = (20, 20); 3P = 2P + P = (14, 14); 4P = 2P + 2P = (19, 20); 5P = 2P + 2P + P = (13, 10); 6P = 2P + 2P + 2P = (17, 32); 7P = 2P + 2P + 2P + P = (18, 72); 8P = 2P + 2P + 2P + 2P = (12, 17); 9P = 2P + 2P + 2P + 2P + P = (4, 5) Here 9P = (4, 5) = Q. Therefore, the value of the discrete logarithm n is 9.	1 1 1 1 1 1 1 1 1 1
7.	Given a text: "VIT" Create the process of deriving eighty 64-bit words from1024 bits for processing of a single message block of SHA-512 . Show the words W16, W17, W18 and W19.	
	Formula for Wt and diagram for message block generation Padding bits: 896 mod 1024 = 896 - 24 = 872 bits, consisting of a "1" bit followed by 871 "0" bit  Initial Block: 56495480.....18 (Hex) or Bin; No, of padding bits: 872 W16= 5649548000000000 (Hex) or Bin W17= 0006000000000780 (Hex) or Bin W18= 201F8EC92A900002 (Hex) or Bin W19= EEO0001800066000 (Hex) or Bin	2 2 2 2 2

8.	Assume Global prime p= 227, generator, α= 14, Alice selected Xa :227, Bob selected Xb :170. Find the public keys of Alice and Bob. Show the scenario of man in the middle attack.	
Ans	a) Alice public key = 14 b) Bob's public key = 101 c) Shared secret Key= 101 d) MIM scenario (diagram with formula)  **Ex:** Eve selected private number for Alice, **Ea : 65**; Eve selected pvt number for Bob, **Eb : 175**. Shared secret key between Alice and Eve: 41 Secret key between Bob and Eve: 167	2 2 2 2 2
9.	In MD5, M= VIT VELLORE; Show the initial message blocks, padding bits and length field. Find the logic functions F,G, H and I only. The buffer values are given: Word A: 10 32 54 76 Word B: ba fe cd 98 Word C: 78 ce ae de Word D: 01 23 45 67	
Ans .	Initial message block, **padding bits:448-88=360; length field: 58H (formulas only: 1 mark)** `F(B,C,D)= 00111001 11001111 10001100 11111111 or` **`39CF8CFF (Hex)`** `G(B,C,D)= 01111000 11101110 11101111 10011000 or` **`78EEEF98 (Hex)`** `H(B,C,D)= 11000011 00010011 00100110 00100001 or` **`C3132621 (Hex)`** `I(B,C,D)= 10000110 00110000 01010001 01000110 or` **`86305146 (Hex)`**	2 2 2 2 2
10.	Given parameters (p,q,g) =(283,47,60) and Alice private key = 24; Hash=H(M)=41. Generate digital signature using DSS and verify the same.	
Ans	DSS - Signing and verification formulas Signing: Verifying: Test v=r $r = (g^k \bmod p) \bmod q$ $w = (s')^{-1} \bmod q$ $u_2 = (r')w \bmod q$ $s = \left[k^{-1}(H(M) + xr)\right] \bmod q$ $u_1 = \left[H(M')w\right] \bmod q$ $v = \left[\left(g^{u1} y^{u2}\right) \bmod p\right] \bmod q$ Signing: Ya= 158; **Let K=15**; then r=19; k^{-1}mod q=22; s= 30 Signature: (r,s) =(19,30) Verifying: w=11; u1=28; u2=21; then v=19; Test v=r ; verified. Note: **As 'k' is not explicitly given, it may be taken the same pvt key value '24' or it may be assumed k<q**	2 4 4
11.	Alice started an online classes and hosted an application. He got a merchant account from national credit card company. He wants to provide payment option with PayPal. What are the various kind of operations that happen with PayPal and in its absence? Suggest your overall opinion to Alice in this scenario with suitable diagrams.	
Ans	Diagrams: 3 marks Explanation: 2 marks  	5 2

	 **Dual Signature:** ***Cryptography operation carried out with Paypal:*** ● *End-to-end encryption is one of many security features that PayPal puts in place to keep customers to make secure transaction ass follows:* ● ***Data encryption.*** *To protect all transactions, PayPal uses 128-bit data encryption Secure Sockets Layer (SSL) protocol technology.* ● ***Application layer security:*** *It uses Secure electronic transaction (SET) protocol to make secure authentication for customer and merchant using dual signature as shown in fig.*	3
12 A)	Consider a banking application to provide MAC and encryption for the electronic transaction. Suggest a suitable protocol with diagrams for this and discuss the Crypto algorithms and steps involved in this electronic fund transfer.	
Ans	TLS Diagram (2 marks) ; Explanation (3marks) 	
12. B	Brief out the future challenges of cyber security	
Ans	**Any 5 points of the following:** Vulnerability scanning, Vulnerability assessment, Preventing open port scanning, **Cybersecurity** is the practice of protecting electronic information by mitigating information risks and vulnerabilities. Information risks can include unauthorized access, use, disclosure, interception, or data destruction. Cyber security is essential to protect businesses and individuals from the potentially devastating consequences of a security breach. In recent years, there have been several high-profile cyberattacks that have had a devastating impact on businesses and individuals. Some of the most common cyberattacks include: **Cyber threats / Attacks/ Vulnerabilities:** Phishing Attacks, Malware attacks, Denial of service attacks, Ransomware Attacks, Man in middle attacks, SQl Injection, Cross site scripting, port scanning, Social engineering, Mobile device vulnerabilities, cloud vulnerabilities, etc. **Cyber threats / Vulnerabilities - Countermeasures:** Confidentiality Integrity Availability (CIA tripod), Cloud Transformation, Vulnerability assessment, port scanning, etc. New technologies -User and Entity Behavior Analytics (UEBA) and Security Orchestration, Automation, and Response (SOAR) are technologies increases the effectiveness of Cyber Security in an organization.	5