EE6102 REVISION 2024

IMPORTANT TOPICS TO FOCUS

- **Cyber security Level**
  - **Current:** Industry 4.0 and digital transformation.
  - **Protection**: Cryptography, firewalls, software updates, use strong passwords and two factor authentication, regular backup, provide regular security training for employees to help them identify potential threats and be cautious when clicking on links or downloading attachments from unknown sources.
  - **Future: ?** However, need to Balance it.
  - **Goals (CIA, Authentication, Privacy, Non-repudiation)**
- **Attacks on cyber security and security threats**
  - Various types of cyber security attacks and attackers
- **PASSWORD SECURITY**
  - Advantages and disadvantages of password-based authentication and biometric-based authentication.
  - **Calculations**: How long it will take to crack a password.
  - In the future, can **biometric** based system be used to replace password-based authentication?

- **Password attacks**: Brute force attacks, dictionary attacks and rainbow table attack.
  - Role of Multi-Factor Authentication (MFA) in cyber security.
- **Phishing Attacks**
  - Various Types of phishing attacks and protection against phishing attacks.
- **Internet of things (IoT) Security:** Role of IoT in launching DDOS attacks. Why attackers are able to recruit many IoT devices to form a Botnet.
- **DOS Attacks**
  - Basic concepts of Denial of service and **DDOS** (distributed denial of service) attacks.
  - SYN flood attack, how it works and how it can be launched.
  - **Calculation:** How many packets are required to launch a DOS attack
  - What is the impact of the packet size?
  - How the speed of the link affects the DOS attack?
  - DNS flood attack?
  - Role of Botnet in DDoS attack

- Malware, Virus, Worms and how to protect against virus attacks.
- Ransomware attacks, Man in the middle attacks.
- **Cyber security compliance, training and awareness**
- **Cyber Security Planning**
  - Two Aspect of Information security (technical and managerial).
  - Security approaches (bottom-up, top-down).
  - **Bottom-Up**: Never succeeds? **Top-down:** Is recombed
- **Cryptography**
  - How encryption provides security and types of encryption (symmetric and asymmetric).
  - Role of a key length.
- **Secrete key cryptography** (Concepts, advantages and disadvantages).
- **Public key cryptography** (concepts, advantages and disadvantages).
- **HASHING**
  - How it provides integrity. Difference between encryption and hashing.
  - We can hash, but Can we de-hash? Use of Hashing in Bitcoin mining.
  - Role of hashing in digital signature (security and efficiency).

- **Digital signature and digital certificate**
  - Digital signature (generating and verifying digital signature, authentication and nonrepudiation).
  - Concept of digital signatures and its use in blockchain technology and cryptocurrencies like Bitcoin and Ethereum.
- **RSA**
  - The algorithm, key generation(e and d), encryption, decryption, RSA security, advantages, disadvantages. The role of large prime numbers in RSA algorithm security.
  - **Calculations:** e, d, encrypt and decrypt message, Digitally sign and verify message using RSA algorithm.
- **DIFFIE-HELLMAN**
  - The algorithm, reasons behind its development, how it works, show how the sender and receiver will receive the same key without compromising the security.
  - Exchanging public key in open and still shared key is secure?
  - **Calculations:** Detailed Calculations of public and shared keys.
  - Ephemeral Diffie-Helman (EDH).
  - Why in TLS 1.3 EDH is used instead of RSA algorithm?

- **Authentication and Authorization**
  - Difference between Authentication and Authorization?
  - Can a user be authorized without an authentication?
- **SSL/TLS AND SET (WEB SECURITY) PROTOCOLS**
  - Differences, Properties, Advantages, Disadvantages.
  - SSL and TLS 1.3 Handshake protocol (with the use of Ephemeral Diffie-Hellman).
  - Major differences between TLS 1.2 and TLS 1.3.
  - How does the use of EDH in TLS1.3 improve the security and efficiency compared to TLS 1.2, which uses RSA for key exchange?
  - Is RSA still used in TLS 1.3? If yes, then for what purpose?
  - The concept of forward secrecy in TLS/SSL protocol and how TLS 1.3 solves this issue?
  - How does SET provide consumer and merchant authentication.
  - SET and SSL use same technology then, why SET failed and SSL became standard for web security?

- **Blockchain Technology, Cryptocurrencies and DeFi.**
  - What was the main reasons for the invention of Bitcoin by Nakamoto?
  - How Blockchain technology provides efficiency, transparency and trust for business applications?
  - How does Blockchain removes the need of intermediaries
  - How does Blockchain provide security, transparency, and immutability.
  - Types of Blockchain technology, its advantages and disadvantages
  - Energy consumption issues in Blockchain technology (Bitcoin mining), its impact on the environment and how to resolve this issue for future blockchain applications
  - Decentralized finance (DeFi) concepts, advantages, disadvantages, risks and the future?
  - How is DeFi challenging the traditional financial system and its current impact on the traditional financial system
  - What role does blockchain technology play in DeFi
  - What is the single main advantage of Blockchain technology?
  - Why cryptocurrencies are volatile?
  - Future of cryptocurrencies, DeFi and blockchain technology?

DIFFIE-HELLMAN EXAMPLE

1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer ***a* = 6**, then sends Bob A = g^a mod p
   - Alice calculates her public key
   - A = 5^6 mod 23 **A = 8** (Alice's Public Key)
3. Bob chooses a secret integer ***b* =15**, then sends Alice B = g^b mod p
   - Bob calculates his public key
   - B = 5^{15} mod 23 **B = 19** (Bob's Public Key)
4. Alice computes her private key **s** = B^a mod p
   - **s** = 19^6 mod 23 **s = 2** (Shared Key)
5. Bob computes his private key **s** = A^b mod p
   - **s** = 8^{15} mod 23 **s = 2** (Shared Key)

- Alice and Bob now share a secret: **s = 2** without compromising the security, as they only exchange public keys over the internet.

RSA EXAMPLE

- Let us select two primes p=11 and q=3
- **Key Generation**
- **n** = p x q = 11x3 = 33
- **ϕ(n)** = (p-1) x (q-1) = 10x2 = **20**
- **Choose Public key e**
  - (p–1) = 11-1 = **10** **(Factors = 2, 5)**
  - (q-1)=3-1= **2** **(Factors = 2)**
  - First 4 Prime numbers: **1, 2, 3, 5**
  - Select **1**: Even though 1 is prime number it is not used. **X**
  - Select **2**: This will have common factors with 10 and 2. **X**
  - Select **3**: This will not have common factors with 10, and 2. √
  - Select **5**: This will have common factors with 10 **X**
- **Compute d**
  - **d = [Kϕ(n) + 1]/e for K =1** **[20+1]/3 = 7**
  - **Public key** = (n, e) = (33, **3**) **Private key** = (n, d) = (33, **7**)

RSA EXAMPLE

- **Public key** = (n, e) = (33, **3**) **Private key** = (n, d) = (33, **7**)
- Let us assume message **M = 8**
- **Encryption**
- **C**=M^e mod n $C = 8^3 \bmod 33 =$ **17** (Cipher text)
- **Decryption**
- **M**=C^d mod n $M = 17^7 \bmod 33 =$ **8** (Plain text)
- **Digital Signature Generation**
- **S** = M^d mod n $S = 8^7 \bmod 33 =$ **2** (generation)
- **Digital Signature Verification**
- **M** = S^e mod n $M = 2^3 \bmod 33 =$ **8** (verification)

DOS ATTACK EXAMPLE

- In a DoS (denial of service) attack packets of **1K word (16-bit)** in size are sent to flood a target organization. Determine the numbers of packets sent by the attacker to launch a successful DoS attack if the speed of the link is 50 Mega bits per second (Mbs). How many numbers of packets would be required if the speed of the link was 100 Mbs.
- The packet size = 1K word (16-bit) = 1024* 16 =16384 bits
- On a 50 Megabit per second (Mbps) link
  - 50000000 / 16384 = 3051.75 packets per second.
  - Thus, the attacker will have to send 3051.75 packets per second to launch a successful attack.
- On a 100 Mbps link
  - 100000000 / 16384 = 6103.5 packets per second.
  - In this case the number of packets required to launch an attack will be= 6103.5 packets per second
- As can be seen, the faster the link, a greater number of packets are required to launch a successful attack.

SHORT QUESTION EXAMPLES

Q: A homeowner has just installed a high-speed cable modem. The homeowner feels that there is no need to worry about security because no one will ever know about their home computer. Explain why should the homeowner be worried about attacks by hackers? What are some of the steps the homeowner should take to secure their home computer?

A: Cable modem is an always-on connection to the Internet making it easier for hackers to find the computer. In addition, some cable modem companies provide their customers with a static IP address. This makes it even easier for hackers to find the computer. Cable modem users can use firewall software to protect their computer. In addition, cable modem users should set their security to a high level.

Q: List some of the basics of choosing a good password.

A: Include at least one capital letter and one lowercase letter in the password

- Mix numbers with letters
- Stay away from passwords that are anywhere near your birthday, last name, spouse's name, too obvious a name, too well known a name, or too common a name
- No dictionary names – hackers have dictionaries
- Change your password often

Model EXAM PAPER

Q 1: Describe symmetric key encryption system including its advantages and limitations. Explain which major problem of symmetric key encryption system is solved by Public key encryption and which dimensions of online security does encryption (PKI) address.

(10 Marks)

Firs read the question carefully and underline the important points required to answer.

Q 1 : Describe symmetric key encryption system including its advantages and limitations. Explain which major problem of symmetric key encryption system is solved by Public key encryption and which dimensions of online security does encryption (PKI) address.

Model EXAM PAPER

Q 1 : Describe symmetric key encryption system including its advantages and limitations. Explain which major problem of symmetric key encryption system is solved by Public key encryption and which dimensions of online security does encryption (PKI) address.

(10 Marks)

A: Symmetric key uses the same shared key to encrypt and decrypt the message.

- **Limitation**
  - For the sender and the receiver to have the same key, it must be sent over a communication media that is insecure, thus, how to exchange the key.
  - If the secret key is lost or stolen, the encryption system fails.
- **Advantages**
  - It can be used effectively for data storage protection
  - Fast, secure and require shorter key
- Public key encryption solves the problem of exchanging keys.
  - In this method every user has a pair of numeric keys: private and public.
  - The keys can only be used in pairs.

- Encryption can provide four key dimensions of e-commerce security.
  - ✓ It can provide assurance that the message has not been altered (**integrity)**
  - ✓ Prevent the user from denying that he/she has sent the message (**nonrepudiation**)
  - ✓ Provide verification of the identity of the message (**authentication**)
  - ✓ Gives assurance that the message has not been read by others (**confidentiality**).

Q 2: For online security, many organizations and individuals use digital signature and hash digests. Explain what dimensions do digital signatures and hash digests add to public key encryption and how do they work? **(5 Marks)**

A:

- Digital signatures and hash digests add authentication, nonrepudiation, and integrity when used with public key encryption.
- The sender encrypts the message using their private key to produce a digital signature.
- To ensure it has not been altered in transit, a hash function is used first to create a digest of the message.

Q 3: Both SSL (Secure Sockets Layer) and SET (Secure Electronic Transaction) protocols were designed for secure web transactions. The SET was tailored and heavily publicized as the credit card approved standard however today, SSL is present in all web browsers while SET has almost disappeared. Discuss SSL and SET protocols, their differences and explain the reasons for SET failure despite it being more secure than SSL?

(10 Marks)

- Secure Socket Layer (SSL) is a method where transactions using a Web browser is encrypted. SSL protects the transmission but does not authenticate the sender. On the other hand, Secure Electronic Transaction (SET) authenticates consumer, merchants and all parties during the transactions.
- Although SET was designed by Visa card, Master card and others it failed to gain popularity. Reasons for this include:
  - Need to install SET software on client computers.
  - Cost and complexity for merchants to offer support for SET compared to low cost and simplicity of the SSL.
  - Client-side certificate distribution logistics.
  - SET was difficult to use while SSL was easy to use and built in all popular browsers.

Issue	Secure Socket Layer (SSL)	Secure Electronic Transaction(SET)
Main Aim	Exchange of Data in an Encrypted form.	Ecommerce Related payment mechanism.
Certification	Two parties exchange certification.	All parties so involved must be certified by third trusted party.
Authentication	Mechanisms in place but not very strong.	Strong mechanism in SET for all parties involved.
Risk of Merchant Fraud	Possible since customer gives Financial details to merchant.	Unlikely as Financial details are given to PAYMENT Gateway.
Risk of Customer fraud.	Possible as no mechanism exist if a customer refuses to pay later.	Customer has to digitally sign payment instructions.
Action in case of customer fraud.	Merchant is Liable.	Payment Gateway is Liable.
Practical Usage	High	Not much.

Q4: Jenifer wants to use RSA algorithm to communicate with Ted. She creates a pair of keys for herself by choosing two prime numbers p =7, q = 11. She also chooses public key, e = 13 and calculates the private key, d= 37. Show how Ted can send the message "y" (24) to Jenifer if he knows the public key, e and can calculate n (7x11= 77). Is any problem if Jenifer chooses e =2 as a public key? **(15 Marks)**

A: P = y=24, e =13, d = 37 and n =77

- $C = P^e \pmod n$, Substituting the values we have
- $C = 24^{13} \bmod 77 = 52$
- When Jenifer receives the encrypted message 52, she uses her private key d= 37 to decode it.
- $M = C^d \pmod n$, Substituting the values we have
- $M = 52^{37} \bmod 77 = 24$, which in this case is "Y".
- If Jenifer chooses, public key *e* = 2, then this will not be RSA, because in RSA, e (public key) must be relatively prime to $\phi(n)$ and less that $\phi(n)$.
- Thus, Jenifer cannot choose public key, e = 2, as this will not fulfil the required condition for RSA algorithm.

Q5: A few computer savvy teenagers are very upset with a local company called ABC and are trying to launch a DoS (denial of service) attack. They are sending packets of 2K bytes in size to company ABC. Determine the numbers of packets sent by the teenage attackers to launch a successful DoS attack on company ABC if the speed of the link is 100 Megabits per second (Mbs). How many numbers of packets would be required if the speed of the link was 150 Mbs. Explain why the number of packets required increases as the speed of the link increases? Clearly state your assumptions (if any). **(15 Marks)**

A: The packet size = 2**K bytes** = 2***1024*** **8** =16384 bits

- On a 100 Megabit per second (Mbps) link
- 100,000,000 / 16384 = 6103.5 packets per second.
- On a 150 Mbps link
- 150,000,000 / 16384 = 9155.2 packets per second.
- As can be seen, the faster the link, a greater number of packets are required to launch a successful attack. This is because higher speed offers larger bandwidth and thus to fill that bandwidth, one must send more packets to launch a successful DOS attack.

Q6: Assume that Bob wants to use RSA algorithm to digitally sign a document and then send it to Alice. Both Alice and Bob have chosen p =3 and q = 11 as two prime numbers and Bob has selected e = 7, as his public key. Bob wants to sign message M= 6 and send it to Alice.

(i) Calculate Bob' private key, d.

(ii) Calculate the digital signature.

(iii) Verify the digital signature

(15 Marks)

A: Given: p =3, q = 11, e = 7 and M= 6

(i)

- $\phi(n) = (p-1)*(q-1) = 2 \times 10 = 20$.
- $n = p*q = 13* 11 = 33$
- Private key d can be calculated as below:
  - $e \times d=1 \pmod{\phi(n)}$
  - $e \times d= k\ \phi(n) +1$.
  - $7 \times d=k\ (20) +1$ For K = 1 we have
  - $d = \{1(20)+1\}/7 = 3$
  - d = 3, Bob's private key = 3

(ii) Calculate the digital signature.

- Digital signature in RSA is given as
  - $S = M^d \pmod{n}$
  - $S = 6^3 \bmod 33 = 18$
  - This is digital signature; which Bob can send to Alice.

(iii) Verify the digital signature

- Alice can verify the digital signature using
  - $M = S^e \pmod{n}$
  - $M = 18^7 \bmod 33 = 6$.
- Since Alice is able to recover the message by decrypting the digital signature using Bob's public key, it is confirmed that it was Bob who has sign it. This verify the digital signature.

Q7: Alice and Bob have agreed to use a prime numbers p=3 and q=7 to generate public and private keys for RSA algorithm.

I. Calculate the first 2 possible public keys

II. Calculate Bob's private key, assuming that he has chosen 5 as his public key

III. Encrypt the message m = 8 and find the ciphertext. **(15 Marks)**

A:

- Given, p =3 and q = 7 as two prime numbers, Bob's Public key, e = 5, Message m= 8
- We calculate: $\phi(n)$ = (p-1)*(q-1) = 2 x 6 = 12 n = p*q = 7* 11 = 21

I.

- (p-1) = 2, which has 2 as its factor
- (q-1) = 6, which has 2 and 3 as its factors
- 1 and 2 cannot be chosen as a public key
- Since (p-1) and (q-1) and 3 have common factors, 3 cannot be chosen as public key.
- Therefore, the first two possible values for public key are: 5 and 7.

II. Private key d can be calculated as below:

- e x d=1 (mod ϕ(n))
- e x d= k ϕ(n) +1
- 5 x d=k (12) +1.
- For K = 1 we have
  - d = {1(12) +1}/5 = 13/5.
  - Since the result is not a whole number, it doesn't satisfy the condition
- For K = 2 we have
  - 5 x d=k (12) +1.
  - d = {2(12)+1}/5 = 5
  - Since it satisfies the condition, it is private key.
  - Bob's private key = 5

III. Encryption in RSA is given as

- $C = m^e \pmod n$
- $C = 8^5 \bmod 21 = 8$
- The ciphertext = 8

Q 8: Describe a SYN flooding attack. Assume that an attacker is launching a DoS (denial of service) attack on an organization, which is using a 500 Megabits/second link. The attacker is sending packets of 256K bytes size. Calculate the numbers of packets the attacker has to send in order to launch a successful DoS attack. How many packets will be required if the attacker is sending packets of 512K bytes and the organization is using a 5 Gigabits/second link. Explain how the size of the packets and the speed of the link effects the number of packets required for launching a successful attack.

(15 Marks)

A: In a TCP SYN flooding attack, an attacker uses bots to flood a server with TCP connection-opening (SYN) requests. A server reserves a certain amount of capacity each time it receives a SYN segment. Flooding a server with SYN segments can cause the server to run out of resources and crash or be unable to open valid requests. A SYN flood can shut down an entire network if strong enough.

- The numbers of packets sent by the attacker to launch a successful DoS attack will depend on speed of the link and the packet size.

- The packet size = 256K bytes = 256*1024* 8 =2,097,152 bits
  - On a 500 Megabit per second (Mbps) link
  - 500,000,000 / 2097152 = 238.418 packets per second.
  - Thus, the attacker will have to send 238.418 packets per second to launch a successful attack.
- Now the speed of the link and the size of the packets has increased.
  - Packet size = 512Kbytes = 512*1024*8 = 4194304 bits
  - On a 5 Gbps link
  - 5,000,000,000 /4194304 = 1192.09 packets per second.
  - In this case the number of packets required to launch an attack will be= 1192.09 packets per second
- As can be seen above, even though the link is faster, the packet size also has doubled. Thus, the actual number of packets required depends on the size of the packets and the speed of the link. If the size of the packets remains the same and the speed of the link is increased, then the number of packets required to launch the successful attack will be increased as well.

Q9: A multinational company is having problems with its password-based security system and is considering using a biometric based authentication system. What biometric systems could the company employ? What are some of the factors it should consider when deciding among various biometric systems? Over the years, it has been claimed that biometric technology can easily replace the password-based authentication used in real digital world and if this is true then why are we still using password for authentication? Explain your answer with proper justification.

(15 Marks)

- The firm could use any available biometric device. Examples include facial feature, fingerprint pattern, iris pattern, hand geometry, vein pattern and speech pattern analysis. What is special about biometrics is that they are the only technologies that can bind an authentication or verification event to an actual person rather than to a name list, a number that is remembered or a token that is carried (like an ID card).
- Fingerprints, retina scans, or speech recognition systems can be used to identify individuals before they can access a Web site or pay for merchandise with a credit card.

- The most popular being fingerprint and retinal scanning. When picking an option, the firm will consider cost, reliability and integration into existing systems.
- Table below shows the comparison of all popular biometric technologies.
- In ideal conditions, biometric systems work quite well, however in real world conditions, their performance is not that great (as shown in table above). The only biometric which is 100% accurate is DNA and no one will be willing to use DNA to replace the password. Therefore, until we have more accurate biometric systems, we will be using password for authentication. If someone knows the user's password, he/she can reset it, however if a biometric is stolen, it cannot be reset.

Method	Coded Pattern	MisIdentific --ation rate	Security	**Applications**
Iris	Iris pattern	1/1,200,000	High	high-security
Fingerprint	fingerprints	1/1,000	Medium	Universal
voice	Voice characteristics	1/30	Low	Telephone service
Signature	Shape of letters, writing Order, pen pressure	1/100	Low	Low-security
Face	Outline, shape & distribution of eyes, nose	1/100	Low	Low-security
Palm	size, length, & thickness hands	1/700	Low	Low-security

Q10: For cryptography it is recommended that the Key must be long, while for password-based authentication, one must choose a long password. Yet most personal identification numbers (PINs) that you type when you use an ATM card are only four or six characters long. Yet this is safe. Why? Explain your answer with proper justification.

(10 Marks)

- Passwords can be entered automatically, and the system can be tricked to allow unlimited attempts. Normally, the attacker will take over millions of compromised computers and with fast connections, this task of cracking a cryptography password can be accomplished within few seconds and the attacker could be sitting in a comfortable and cozy environment.
- The ATM card's PINs must be entered manually, which is a slow process. Even with only four-number PINs, it would take an attacker a long amount of time to try enough combinations to succeed. After three unsuccessful attempts, ATM card will be taken by the machine.
- Since the attacker must be physically present at an ATM machine, if caught, the local law will apply, and the attacker will be punished.
- For the above reasons, it is easy for attackers to crack long passwords, compared to short ATM pins.

Q11: Briefly explain the below security services desired in cyber security. For each service, explain what the service means and how cryptography (including digital signature) can be used to achieve the desired goals. Authentication, Confidentiality, Integrity, Non-repudiation

(10 Marks)

- Authentication: Assure message and communicating parties are authenticated. Using digital signature, sender can be authenticated and since private key is kept confidential, it is better for online authentication compared to password.
- Confidentiality: It means that people cannot read sensitive information. Using cryptography, the message can remain confidential between the sender and receiver.
- Integrity: It means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Using cryptography, integrity of the data can be protected.
- Non-repudiation: Prevent sender or receiver from denying that communications took place. This can be achieved with the use of digital signature. In this case the sender cannot deny the communication, as he/she has digitally signed the message using her/his private key.

Q12: Describe Blockchain technology, including its major types.

(10 Marks)

- Blockchain technology is a decentralized and distributed digital ledger that records transactions in a secure and tamper-proof way. The technology uses cryptographic algorithms to validate and verify transactions, creating a permanent and immutable record that is accessible to all network participants.

- The major types of blockchain technology are:

1. Public Blockchain: A public blockchain is open to everyone and allows anyone to participate in the network. Bitcoin and Ethereum are examples of public blockchains.

2. Private Blockchain: A private blockchain is restricted to a specific group of participants, and access is controlled by a central authority. Private blockchains are often used by businesses and organizations for internal purposes.

3. Consortium Blockchain: A consortium blockchain is a type of private blockchain where the participants are known and trusted. Consortium blockchains are often used in industries such as finance, supply chain, and healthcare.

Q13: What is DeFi? Describe its advantages, disadvantages and possible future prospectus?

(10 Marks)

- DeFi, or Decentralized Finance, refers to a new movement within the cryptocurrency and blockchain industry that seeks to provide traditional financial services such as lending, borrowing, and trading, using decentralized protocols and applications that operate on public blockchain networks.
- Advantages of DeFi: Decentralization (resistant to censorship and single points of failure), Transparency, Accessibility and Lower Costs (can provide financial services at a lower cost than traditional financial institutions, as they do not require intermediaries).
- Disadvantages of DeFi: Volatility (Cryptocurrencies are highly volatile and can lead to sudden price drops, which could result in a loss of funds), Security (susceptible to hacks and exploits as the platforms are not regulated), Complexity (for those who are not familiar with the cryptocurrency and blockchain industry).
- Future Prospectus: Overall, DeFi has the potential to revolutionize the financial industry by providing greater financial access and inclusivity.