NADAR SARASWATHI COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY

2

MARK QUESTIONS & ANSWERS

YEAR / SEMESTER*: IV / VII*

REGULATION: *2013*

2018 - 2019

CS6701 CRYPTOGRAPHY AND NETWORK SECURITY

2 Mark Questions & Answers

UNIT-I INTRODUCTION & NUMBER THEORY

1. What is meant by cryptography and cryptanalysis? (N/D-09)

Cryptography is an art of writing hidden messages. It is a historical (or) forensic approach. Cryptanalysis is the process of analyzing hidden messages. It is a statistical (or) analytical approach.

2. What are the key principles of security? (A/M-12)

The key principle of security is the following:

1. Make sure you have the latest security updates & patches
2. Install anti-virus software
3. Install anti-spyware software
4. Use a personal firewall
5. Password advice

3. Differentiate conventional (symmetric) from public key (asymmetric) encryption. (M/J-07)

Conventional Encryption	**Public-Key Encryption**
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.	Needed to work: 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not of the same one).
Needed for Security: 1. The key must be kept secret. 2. It must be impossible or atleast impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	Needed for security: 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of the ciphertext must be insufficient to determine the other key.

4. Distinguish between passive attack and active attack with reference to X.800. (A/M-11)

X.800 categorize the attacks into two, namely passive and active attacks.

Passive attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. It includes release of message contents and Traffic analysis. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks, usually by means of encryption.

Active attacks: Active attack involves some modification of the data stream or the creation of a false data stream and can be subdivided into four categories namely as a masquerade, replay, modification of messages and the denial of service attack.

5. Define – Key and Plaintext (M/J-09)

In cryptography, a key is defined as a piece of information that determines the functional output of a cryptographic algorithm or cipher. In encryption, a key specifies the particular transformation of plaintext into ciphertext or vice versa during decryption. Plaintext is ordinary readable text before being encrypted into ciphertext or after being decrypted.

6. Find the GCD of 2740 and 1760, using Euclidean algorithm. (N/D-08)

The GCD of two numbers say *a* and *b* can be found using the following formula

gcd(a,b) =gcd(b,a mod b)

GCD(2740,1760) = gcd(1760, 2740 mod 1760)= gcd(1760,980)=980

7. What is encipherment? (A/M-12)

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

8. What is a passive attack? (M/J-09)

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

9. What is the difference between a monoalphabet cipher and a polyalphabetic cipher? (A/M-12)

Monoalphabetic cipher is a monoalphabetic cipher is a substitution cipher in which the cipher alphabet is fixed through the encryption process. All of the substitution ciphers we have seen prior to this handout are monoalphabetic; these ciphers are highly susceptible to frequency analysis. Polyalphabetic Cipher is a polyalphabetic cipher is a substitution cipher in which the cipher alphabet changes during the encryption process.

10. What is the avalanche effect? (M/J-07)

In cryptography, the avalanche effect refers to a desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions. The avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.

UNIT-II BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

1. Prove that 3 is a primitive root of 7. (M/J-07)

That is, if is a primitive root of the prime number, then the numbers

a mod p, a^2 *mod p,…* a^{p-1} *mod p*

3 mod 7, 9 mod 7, 27 mod 7, …. 656 mod 7

3, 2, 6,…..5.

2. Write any one technique of attacking RSA. (A/M-11)

The most widely used public-key cryptosystem is RSA. The difficulty of attacking RSA is based on the difficulty of finding the prime factors of a composite number.

THE FACTORING PROBLEM: We can identify three approaches to attacking RSA mathematically.

1. Factor *n* into its two prime factors .This enables calculation of *Ø(n) =(p-1)x(q-1)* ,which in turn enables determination of $d \equiv e^{-1}$ *(mod Ø(n)).*
2. Determine *Ø(n)* directly, without first determining *p* and *q*. Again, this enables determination of $d \equiv e^{-1}$ *(mod Ø(n)).*
3. Determine *d* directly, without first determining *Ø(n).*

3. What is differential cryptanalysis? (N/D-08)

Differential cryptanalysis is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting ciphertext provide information that can be used to determine the encryption key.

4. What is linear cryptanalysis? (A/M-12)

This attack is based on finding linear approximations to describe the transformations performed in DES. This method can find a DES key given 2^{43} known plaintexts, as compared to 2^{47} chosen plaintexts for differential cryptanalysis. Although this is a minor improvement, because it may be easier to acquire known plaintext rather than chosen plaintext, it still leaves linear cryptanalysis infeasible as an attack on DES. So far, little work has been done by other groups to validate the linear cryptanalytic approach.

5. What are the requirements for the use of a public-key certificate scheme? (M/J-09)

Four requirements can be placed on this particular scheme:

1. Any participant can read a certificate to determine the name and public key

of the certificate's owner

2. Any participant can read a certificate to determine the name and public key of the certificate's owner
3. Only the certificate authority can create and update certificates
4. Any participant can verify the currency of the certificate

6. What are the different modes of operation in DES? (A/M-11)

1. Double DES
2. Triple DES
3. Electronic Code Book
4. Counter mode
5. Cipher block chaining mode
6. Cipher Feedback mode

7. What are the CFB and OFB modes? (M/J-07)

The Cipher Feedback (CFB) mode and the Output Feedback (OFB) mode are two standard modes of operation a block cipher.

In CFB mode the previous ciphertext block is encrypted and the output produced is combined with the plaintext block using exclusive-or to produce the current ciphertext block. OFB mode is similar to the CFB mode except that the quantity exclusive-oared with each plaintext block is generated independently of both the plaintext and ciphertext.

8. What is DES? (M/J-09)

Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations.

9. Compare the symmetric and asymmetric key cryptography. (A/M-12)

Symmetric Encryption uses a single secret key that needs to be shared among the people who needs to receive the message while Asymmetric encryption uses a pair of public key, and a private key to encrypt and decrypt messages when communicating.

1. Symmetric Encryption is an age old technique while asymmetric Encryption is relatively new.

2. Asymmetric Encryption was introduced to complement the inherent problem of the need to share the key in symmetric encryption model eliminating the need to share the key by using a pair of public-private keys.

10. What are the disadvantages of double DES? (N/D-12)

The following are the disadvantages of double DES

1. Reduction to a single stage. \
2. Meet in the middle attacks.
3. Double DES is less secure than triple DES.
4. Double DES is within brute force attack.

UNIT-III HASH FUNCTIONS AND DIGITAL SIGNATURES

1. What is meant by the Diffie-Hellman key exchange? (A/M-12)

An element g is called a generator of a group G if every element in G can be expressed as the product of finitely many powers of g.

If p≥1 is an integer, then the numbers coprime to p, taken modulo p, form a group with multiplication as its operation. It is written as (Z/pZ)×or Zp*.

2. How does Diffie-Hellman key exchange achieve security? (N/D-08)

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

3. What is weak collision resistance? What is the use of it? (M/J-13)

For any given block x, It is computationally infeasible to find $Y \neq X$ with $H(Y) \neq H(X)$. It guarantees than an alternative message hashing to the same value as a given message cannot found. This prevents forgery when as encrypted hash code is used.

4. What is meant by EIGamal cryptosystem? (A/M-11)

The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.

5. What is meant by one-way property in hash function? (A/M -11)

For any given code h, it is computationally infeasible to find X such that $H(x) = h$. A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

6. List out the requirements of kerberos. (A/M -11)

The requirements of Kerberos are as follows:

(1) Secure (2) Reliable (3) Transparent (4) Scalable

7. What is meant by life cycle of a key? (A/M-12)

Keys have limited lifetimes for a number of reasons. The most important reason is protection against cryptanalysis. Each time the key is used, it generates a number of ciphertexts. Using a key repetitively allows an attacker to build up a store of ciphertext (and possibly plaintexts) which may prove sufficient for a successful cryptanalysis of the key value. If you suspect that an attacker may have obtained your key, then your key is considered compromised.

8. What is a hash function? (N/D-09)

A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.

9. What are the types of attacks addressed by message authentication?

There are four types of message authentication:

1. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or no receipt by someone other than the message recipient.
2. Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
3. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
4. Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

10. What are two levels of functionality that comprise a message authentication or digital signature mechanism?

At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower-level function is then used as primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

11. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be computationally secure if: (1) the cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.

12. What is the difference between a message authentication code and a one-way hash function? (N/D-09)

A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

UNIT-IV SECURITY PRACTICE & SYSTEM SECURITY

1 .Why does PGP generate a signature before applying compression? (A/M-11)

The signature is generated before compression due to 2 reasons:

It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future.

2. Write the four SSL Protocols. (A/M-11)

1. SSL Handshake protocol
2. SSL Change cipher spec. protocol
3. SSL Alert Protocol
4. SSL Record Protocol

3. What is meant by S/MIME? (A/M-12)

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME is on an IETF standards track and defined in a number of documents, most importantly RFCs (3369, 3370, 3850, 3851). S/MIME was originally developed by RSA Data Security Inc. The original specification used the IETF MIME specification with the de facto industry standard PKCS secure message format. Change control to S/MIME has since been vested in the IETF and the specification is now layered on cryptographic message syntax.

4. What are the services provided by IPSec? (N/D-09)

The services provided by IPSec are authentication, confidentiality and key management authentication. It ensures the identity of an entity. Confidentiality is protection of data from unauthorized disclosure. Key management is generation, exchange, storage, safeguarding, etc. of keys in a public key cryptography.

5. What is meant by replay attack? (A/M-11)

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

6. What is the difference between an SSL connection and SSL session? (M/J-09)

Connection is a transport that provides a suitable type of service. For SSL, such connections are peer-topeer relationships. The connections are transient. Every connection is associated with one session. Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

7. Why does ESP include a padding field? (N/D-08)

The ciphertext needs to end on an eight octet boundary because the Authentication data field is properly aligned in the packet. This is what the protocol expects and if it doesn't follow the rules, it's considered to contain an error in the packet. It's like English or other languages. We expect sentences to end with a period so we know where one sentence ends and the other begins.

8. What is the problem that kerberos addresses? (A/M-12)

The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment a workstation cannot be trusted to identify its users correctly to network services.

9. What is meant by the function of a compression function in a hash function?

The hash function involves repeated use of a compression function. The motivation is that if the compression function is collision resistant, then the hash function is also collision resistant function. So a secure hash function can be produced.

10. How is signed data entity of S/MIME prepared?

Secure/Multipurpose Internet Mail Extension is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA data security. It is able to sign and/or encrypt messages.

11. What are the services provided by IPSec?

1. Access control
2. Connectionless integrity
3. Data origin authentication
4. Rejection of replayed packets

12. List out four requirements defined for kerberos. (M/J-09)

The four requirements defined for Kerberos are:

1. Secure: A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally Kerberos should be strong enough that a potential opponent does not find it to be the weak link.
2. Reliable: For all services that relay on Kerberos for access control, lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ distributed server architecture, with one system able to back up another.
3. Transparent: Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password.
4. Scalable: The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

13. What are the entities that constitute a full-service kerberos environment? (N/D-08)

A full service environment consists of a Kerberos server, a number of clients and a number of application servers.

14. What is the need of segmentation and reassembly function in PGP?

E-mail facilities often are restricted to a maximum message length. To accommodate this restriction, PGP automatically subdivides a message that is too large into segments that are small enough to send via e-mail. The segmentation is done after all of the other processing, including the radix-64 conversion. Thus, the session key component and signature component appear only once, at the beginning of the first segment.

UNIT-V E-MAIL, IP & WEB SECURITY

1. Define – Virus (A/M-12)

Computer Viruses is defined as the malicious software programs that damage computer program entering into the computer without the permission of the users, and also run against the wishes of the users. They are replicated by themselves. Viruses are so dangerous and malicious that they can be automatically copied and pasted from memory to memory over and over.

Types of virus:

Boot sector Virus
Macro virus
Multipartite Virus
Stealth virus

2. What is application level gateway? (A/M-11)

An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

3. List out the design goals of firewalls. (M/J-09)

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
3. The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system.

4. What is meant by intrusion detection system? (N/D-08)

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

5. What are audit reports? Writ its two forms. (N/D-09)

An information security audit is an audit on the level of information security in an organization. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits, etc. Most commonly the controls being audited can be categorized to technical, physical and administrative. Auditing information security covers topics from auditing the physical security of data centers to auditing the logical security of databases and highlights key components to look for and different methods for auditing these areas.

6. Define − Password Protection (A/M-12)

Password protection is defined as a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

7. Define − Malicious Program (M/J-07)

Malicious software is defined as a software written with the intent of causing some inconvenience to the user of the software. Malicious software in general terms is quite often called a virus however there are many other forms of malicious software. Some other types of malicious or potentially malicious software are worms, trojan horses, spyware, and PuPs.

8. What is meant by intruder? (A/M-12)

A network is accessed by unauthorized user is called intrusion and the user is called as intruder.

Classes of intruders:

Masquerader
Misfeasor
Clandestine user

9. What is meant by worm?

A computer worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code. Worms utilize networks to send copies of the original code to other computers, causing harm by consuming bandwidth or possibly deleting files or sending documents via email. Worms can also install backdoors on computers.

10. What is meant by Trojan horse?

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

11. What is meant by logic bomb?

A logic bomb is a malicious program timed to cause harm at a certain point in time, but is inactive up until that point. A set trigger, such as a preprogrammed date and time, activates a logic bomb. Once activated, a logic bomb implements a malicious code that causes harm to a computer. A logic bomb, also called slag code.

12. What are the steps in virus removal process? (N/D-09)

Virus should be removed form the system by scanning process. The steps include in this process are,

1. Backup your data
2. Check to ensure that other factors aren't causing your problem
3. Gather your antivirus tools
4. Reboot in Safe Mode
5. Run your scans
6. Test your computer

13. What is meant by generic decryption technology? (A/M-12)

A generic decryption technology can detect most complex polymorphic viruses with fast scanning speed.

14. What is meant by denial of service?

A denial of service is an attempt to prevent a genuine user of service from using it. A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include,

- Attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to prevent a particular individual from accessing a service.
- Attempts to disrupt service to a specific system or person.