CS707 – Network Security Midterm Paper

Q1 _____ is a symmetric block cipher, uses a 64 bit key, puts the data through 16 rounds of transposition and substitution, and has 5 different modes of operation.

- AES
- DES
- Blowfish
- None of above

Q2 Examples of asymmetric key algorithms are:

- Diffie Hellman, RSA and El-Gamal
- RC4, RC5, and RC6
- DES, 3DES, and AES
- MD4, MD5, and MD6

Q3 The standard used in digital certificates that defines its structure, fields, and values is

- Kerberos
- End-to-end encryption
- X.509
- The standard used in IPSEC VPNs

Q4 A cryptosystem consists of:

- Software, algorithms, protocols, and keys
- PGP
- An algorithm used for encryption and decryption
- Is software used for testing security of applications

Q5 Cryptanalysis is:

- The practice of analyzing secret codes but not breaking them
- The technique used by forensic investigators to trace the source of malware infection
- The science related to research and development of cryptography
- The practice of breaking cryptic systems

Q6 An electro-mechanical cipher machine used by the Germans in World War II is _____

- MAC
- Enigma
- Skytale
- All above

Q7 A digital signature is best described as:

- An electronic verification system used for transactional integrity in banking
- A hash value encrypted by the sender's private key
- An electronic verification system used for encryption and hashing
- A hash value encrypted with the DES, 3DES, or AES algorithms

Q8 A practice of Choosing a key that is extremely random and the algorithm should use the full range of the key-space is called _____.

- Cipher management
- Key combination
- Key management
- None of above

Q9 _____ uses two instances of the same key while encrypting and decrypting messages.

- Skytale
- Symmetric Cryptography
- Asymmetric Cryptography
- SSL

Q10 _____ is a program and protocol used to log in securely to another device or system on a network.

- Secure Shell (SSH)
- SSL
- HTTP
- PGP

Q11 In Network Security CIA stands for:

- Confidentiality, integrity, and. availability
- Central Investigation Agency
- Confidentiality, Intelligence, and Accountability
- Ciphers, Initiation Vectors, Algorithms

Q:12 Examples of asymmetric key algorithms are:

- Diffie Hellman, RSA and El-Gamal
- RC4, RC5, and RC6
- DES, 3DES, and AES
- MD4, MD5, and MD6

Q:13 A mathematical function that is easier to compute in one direction than in the other direction, and forms the basis for all asymmetric algorithms

- One-Way Function
- Two Way Function
- A mathematical function used in cryptanalysis
- A technique used by forensic experts to lock all hard disk sectors of a computer

Q:14 A hash value encrypted by the sender's private key is _____

- AES
- Digital signature
- DES
- 3DES algorithms

Q:15 Cryptanalysis is:
The practice of analyzing secret codes but not breaking them

- The technique used by forensic investigators to trace the source of malware infection
- The science related to research and development of cryptography
- The practice of breaking cryptic systems

Q:16 Key management is a practice that requires:

- Choosing a key that is extremely random and the algorithm should use the full range of the key-space
- Labeling keys so that they are not lost or stolen
- Returning the key to the CA after it has completed its lifetime
- At least two senior officers of the company to issue and maintain a record of the keys

Q:17 In end-to-end encryption:

- only the header is encrypted, not the payload
- Packets do not need to be decrypted and then encrypted at each hop
- Only decryption takes place at each hop
- The data link and physical layers are involved

Q:18 Rootkits are a type of _____.

- Virus
- Worm.
- Trojan Horse
- None of above

Q:19 Diffie Hellman is an example of _____ key algorithms.

- Symmetric
- Asymmetric
- Skytale
- Enigma

Q:20 The standard used in digital certificates that defines its structure, fields, and values is _____.

- X.509
- Kerberose
- Cryptography
- PKI

2. In context of hashing what is meant by compression.

Compression must occur before encryption, because compression is inefficient on encrypted data: compression algorithms work on detecting redundancies and structure in the data, and encryption is designed to hide redundancies and structure. Basically, compression does not work at all on properly encrypted data. Conversely, if compression works on encrypted data, then the encryption layer should be viewed with deep suspicion...

When hashing occurs in PGP, it is as part of a signature algorithm, or as an integrity check which is generally known as a MAC. There are several ways to do a MAC; the theoretical "good" way is to apply the MAC on the encrypted data. However, PGP dates from an older time where theory was not yet fully worked out, and uses a hash value (i.e. a function which as no key) and then includes the hash in the encrypted data (see section 5.13); the hash value is turned into a MAC by virtue of reusing the encryption key. In the case of such a MAC, the MAC (i.e. the underlying hash) occurs on whatever is encrypted, so that's the compressed data (if compression was used at all). Since you talk about compression "between" the hash and the encryption, then I suppose that you are not talking about that hash at all.

Compressing a sequence of characters drawn from an alphabet uses string substitution with no a priori information. An input data block is processed into an output data block comprised of variable length incompressible data sections and variable length compressed token sections. Multiple hash tables are used based on different subblock sizes for string matching, and this improves the compression ratio and rate of compression. The plurality of uses of the multiple hash tables allows for selection of an appropriate compression data rate and/or compression factor in relation to the input data. Using multiple hashing tables with a recoverable hashing method further improves compression ratio and compression rate. Each incompressible data section contains means to distinguish it from compressed token sections.

3. What is X.509 standard?

PKI is an ISO authentication framework that uses public key cryptography and the X.509 standard.
In cryptography, **X.509** is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
The standard for how the CA creates the certificate is X.509, which dictates the different fields used in the certificate and the valid values that can populate those fields
We are currently at version 4 of this standard, which is often denoted as X.509v4. Many cryptographic protocols use this type of certificate, including SSL.
The certificate includes the serial number, version number, identity information, algorithm information, lifetime dates, and the signature of the issuing authority.

4. What are one way functions? How they are implemented in cryptography?

A one-way function is a mathematical function that is easier to compute in one direction than in the opposite direction.
An analogy of this is when you drop a glass on the floor. Although dropping a glass on the floor is easy, putting all the pieces back together again to reconstruct the original glass is next to impossible.

This concept is similar to how a one-way function is used in cryptography, which is what the RSA algorithm, and all other asymmetric algorithms, is based upon.
The **easy direction of computation** in the one-way function that is used in the RSA algorithm is the process of multiplying two large prime numbers.

Multiplying the two numbers to get the resulting product is much easier than factoring the product and recovering the two initial large prime numbers used to calculate the obtained product, which is the difficult direction.
RSA is based on the difficulty of factoring large numbers that are the product of two large prime numbers.
Attacks on these types of cryptosystems do not necessarily try every possible key value, but rather try to factor the large number, which will give the attacker the private key.

When a user encrypts a message with a public key, this message is encoded with a one-way function (breaking a glass). This function supplies a **trapdoor** (knowledge of how to put the glass back together), but the only way the trapdoor can be taken advantage of is; if it is known about and the correct code is applied. The private key provides this service.

The **private key** knows about the trapdoor, knows how to derive the original prime numbers, and has the necessary programming code to take advantage of this secret trapdoor to unlock the encoded message (reassembling the broken glass). Knowing about the trapdoor and having the correct functionality to take advantage of it are what make the private key private.

When a one-way function is carried out in the easy direction, encryption and digital signature verification functionality are available. **When the one-way function is carried out in the hard direction,** decryption and signature generation functionality are available.

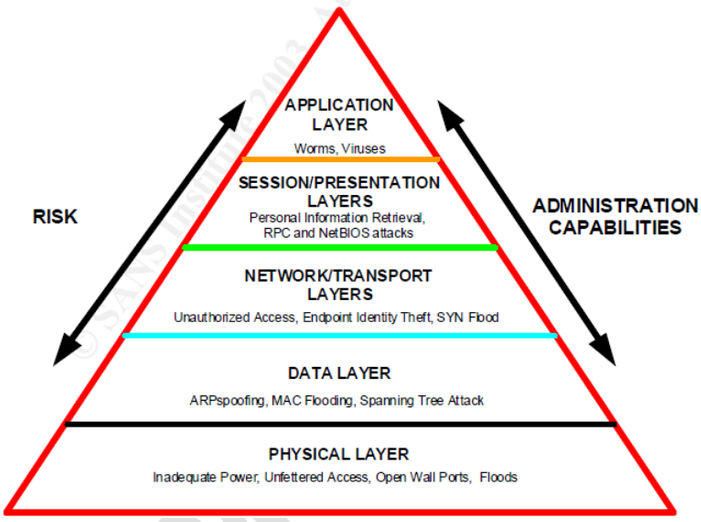
This means only the public key can carry out encryption and signature verification and only the private key can carry out decryption and signature generation.

6. What security measures are adopted in the layers of OSI Model.

In the OSI model approach, security is addressed at each layer of the OSI model, shown below. By comparing in depth the OSI model with the concept of Application Security by Defense, IT managers better understand that securing enterprise application is more than authentication, encryption, OS hardening, etc. At each level of the OSI model there are

Security vulnerabilities and, therefore, security prevention measures that can be taken to ensure that enterprise applications are protected. Importantly, the capability IT managers have to mitigate risks decreases at the higher OSI model layers.

Figure: OSI Pyramid



One reason IT managers have less power to protect applications at the higher OSI layers is that at these higher layers, developers have much more influence over security measures.
However, security measures are possible at every OSI layer. Addressing security threats at every layer reduces the risk of enterprise application compromise or Denial of Service.
Examples of vulnerabilities and solutions at each layer provide a better understanding of the topics presented.

Risks/Attacks and their Measures

The OSI **Physical layer** represents physical application security, which includes access control, power, fire, water, and backups. Many of the threats to security at the Physical layer cause a Denial of Service (DoS) of the enterprise application, making the application unavailable to enterprise users.
Physical locks, both on equipment and facilities housing the equipment, are imperative to keep intruders out. In order to use information one must have access to it. Security cables on laptops and system cases with power button locks are examples of procuring equipment with physical security capabilities.

The Data, or **Data Link, layer** of the OSI model encompasses switch security topics such as ARP spoofing, MAC flooding and spanning tree attacks.

Simple configuration changes to the network switch can help protect enterprise applications from Data layer attacks.
The **Network and Transport layers**of the OSI model are where the most common security precautions take place— this layer is where routers and firewalls are implemented. Threats that occur at this level are unauthorized retrieval of endpoint identity, unauthorized access to internal systems, SYN flood attacks and “ping of death.”

Implementing Network Address Translation, Access Control Lists, and firewall technologies mitigates these risks.
The **Session and Presentation layers** are the lower layers of the Application Set of the OSI model. At these layers the IT manager’s ability to mitigate application security risk begins to diminish as developers take a bigger role in protecting applications.

IT managers can prevent unauthorized login/password accesses and unauthorized data accesses, which are common attacks at these layers, by using encryption and authentication methods.

The **Application layer** is the final layer of the Application Set and the OSI model. Many security protection methods are the responsibility of the programmer at this layer. Backdoor attacks occur at this level and it is the programmer's responsibility to close those doors.

IT managers can use access control methods described to assist in preventing backdoor attacks; also, IT managers can set up tools such as virus scanners, WebInspect, and intrusion detection devices to help prevent compromise of enterprise applications.

7. Define and discuss various components of PKI infrastructure.

The comprehensive system required to provide public-key encryption and digital signature services is known as a public-key infrastructure. The purpose of a public-key infrastructure is to manage keys and certificates. By managing keys and certificates through a PKI, an organization establishes and maintains a trustworthy networking environment. A PKI enables the use of encryption and digital signature services across a wide variety of applications.

A PKI may be made up of the following entities and functions:

- CA(Certificate Authority)
- RA(Registration Authority)
- Certificate repository
- Certificate revocation system
- Key backup and recovery system
- Automatic key update&Management of key histories
- Timestamping
- Client-side software

The detail of each component is as follows:

1. **CA (Certificate Authority)**

A CA is a trusted organization (or server) that maintains and issues digital certificates. When a person requests a certificate, the registration authority (RA) verifies that individual's identity and passes the certificate request off to the CA.

The CA constructs the certificate, signs it, sends it to the requester, and maintains the certificate over its lifetime.

When another person wants to communicate with this person, the CA will basically vouch for that person's identity

2. **RA (Registration authority)**

The registration authority (RA) performs the certification registration duties. The RA establishes and confirms the identity of an individual, initiates the certification process with a CA on behalf of an end user, and performs certificate life-cycle management functions.

The RA cannot issue certificates, but can act as a broker between the user and the CA. When users need new certificates, they make requests to the RA, and the RA verifies all necessary identification information before allowing a request to go to the CA.

3. **Certificate repository**

Certificate repositories store certificates so that applications can retrieve them on behalf of users. The term repository refers to a network service that allows for distribution of certificates.Over the past few years, the consensus in the information technology industry is that the best technology for certificate repositories is provided by directory systems that are LDAP (Lightweight Directory Access Protocol)-compliant.

4. **Certificate revocation system**

Certificates that are no longer trustworthy must be revoked by the CA.There are numerous reasons why a certificate may need to be revoked prior to the end of its validity period. For instance, the private key (that is, either the signing key or the decryption key) corresponding to the public key in the certificate may be compromised. Alternatively, an organization's security policy may dictate that the certificates of employees leaving the organization must be revoked. In these situations, users in the system must be informed that continued use of the certificate is no longer considered secure. The revocation status of a certificate must be checked prior to each use. As a result, a PKI must incorporate a scalable certificate revocation system. The CA must be able to securely publish information regarding the status of each certificate in the system. Application software, on behalf of users, must then verify the revocation information prior to each use of a certificate. The combination of publishing and consistently using certificate revocation information

constitutes a complete revocation system.

CRL: The most popular means for distributing certificate revocation information is for the CA to create secure certificate revocation lists (CRLs) and publish these CRLs to a directory system. CRLs specify the unique serial numbers of all revoked certificates. Prior to using a certificate, the client-side application must check the appropriate CRL to determine if the certificate is still trustworthy. Client-side applications must check for revoked certificates consistently and transparently on behalf of users.

5. Key backup and recovery system

To ensure users are protected against loss of data, the PKI must support a system for backup and recovery of decryption keys. With respect to administrative costs, it is unacceptable for each application to provide its own key backup and recovery. Instead, all PKI-enabled client applications should interact with a single key backup and recovery system. The interactions between the client-side software and the key backup and recovery system must be secure, and the interaction method must be consistent across all PKI-enabled applications.

6. Key update and management of key histories:

Cryptographic key pairs should not be used forever. They must be updated over time. As a result, every organization needs to consider two important issues:

Updating users' key pairs, and Maintaining, where appropriate, the history of previous key pairs.

Updating users' key pairs: The process of updating keys pairs should be transparent to users. This transparency means users do not have to understand that key update needs to take place and they will never experience a "denial of service" because their keys are no longer valid. To ensure transparency and prevent denial of service, users? key pairs must be automatically updated before they expire.

Maintaining histories of key pairs: When encryption key pairs are updated, the history of previous decryption keys must be maintained. This "key history" allows users to access any of their prior decryption keys to decrypt data. (When data is encrypted with a user's encryption key, only the corresponding decryption key—the paired key—can be used for decrypting). To ensure transparency, the client-side software must automatically manage users? histories of decryption keys.

7. Timestamping

Trusted Timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one — not even the owner of the document — should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.

The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect, process and renew timestamps

8. Client-side software

A consistent, easy-to-use PKI implementation within client-side software lowers PKI operating costs. In addition, client-side software must be technologically enabled to support all of the elements of a PKI discussed earlier in this paper. The following list summarizes the requirements client-side software must meet to ensure that users in a business receive a usable, transparent (and thus, acceptable) PKI.

9. Support for Non-repudiation

Repudiation occurs when an individual denies involvement in a transaction. (For instance, when someone claims a credit card is stolen, this means that he or she is repudiating liability for transactions that occur with that card anytime after reporting the theft).

Non-repudiation means that an individual cannot successfully deny involvement in a transaction. In the paper-world, individuals' signatures legally bind them to their transactions (for example, credit card charges, business contracts …). The signature prevents repudiation of those transactions. In the electronic world, the replacement for the pen-based signature is a digital signature. All types of electronic commerce require digital signatures because electronic commerce makes traditional pen-based signatures obsolete.

8. Why Symmetric Key encryption Algorithm is used in an organization. Give its advantages and draw backs.

Strengths (Advantages)

- Much faster (less computationally intensive) than asymmetric systems
- Hard to break if using a large key size

Weaknesses (Drawbacks)

- Requires a secure mechanism to deliver keys properly
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming
- Provides confidentiality but not authenticity or nonrepudiation

9. Enlist 5 modes of DES

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter Mode (CTR)

10. Give Five examples of symmetric Algorithms.

- Data Encryption Standard (DES)
- Triple-DES (3DES)
- Blowfish
- IDEA (International Data Encryption Algorithm)
- RC4, RC5, and RC6
- Advanced Encryption Standard (AES)

11. Write essential ingredients of Symmetric Ciphers.

- Plaintext
- Encryption algorithm
- Secret key
- Cipher text

12. Discuss the strength of Cryptosystem on basis of different parameters 10

- The strength of an encryption method comes from the algorithm, the secrecy of the key, the length of the key, the initialization vectors, and how they all work together within the cryptosystem.
- When strength is discussed in encryption, it refers to how hard it is to figure out the algorithm or key, whichever is not made public.
- The strength of an encryption method correlates to the amount of necessary processing power, resources, and time required to break the cryptosystem or to figure out the value of the key.
- Breaking a cryptosystem can be accomplished by a brute force attack, which means trying every possible key value until the resulting plaintext is meaningful
- Depending on the algorithm and length of the key, this can be an easy task or one that is close to impossible
- The goal when designing an encryption method is to make compromising it too expensive or too time-consuming
- Another name for cryptography strength is **work factor,** which is an estimate of the effort and resources it would take an attacker to penetrate a cryptosystem
- Important elements of encryption are to use an algorithm without flaws, use a large key size, use all possible values within the keyspace, and to protect the actual key.

If one element is weak, it could be the link that dooms the whole process.Even if a user employs an algorithm that has all the requirements for strong encryption, including a large keyspace and a large and random key value, if he shares his key with others, the strength of the algorithm becomes almost irrelevant.

13. Explain the working of DES (Long) 10

How Does DES Work ?

- DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of ciphertext come out.
- It is also a symmetric algorithm, meaning the same key is used for encryption and decryption.
- It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity.
- When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time.
- The blocks are put through 16 rounds of transposition and substitution functions.
- The order and type of transposition and substitution functions depend on the value of the key used with the algorithm.
- The result is 64-bit blocks of ciphertext.

14. What Does It Mean When an Algorithm Is Broken?

- In most instances, an algorithm is broken if someone is able to uncover a key that was used during an encryption process.
- So let's say Ali encrypted a message and sent it to Bilal. Zaheer captures this encrypted message and carries out a brute force attack on it, which means he tries to decrypt the message with different keys until he uncovers the right one.
- Once he identifies this key, the algorithm is considered broken. So does that mean the algorithm is worthless?
- If an algorithm is broken through a brute force attack, this just means the attacker identified the one key that was used for one instance of encryption.
- But in proper implementations, we should be encrypting data with session keys, which are good only for that one session. So even if the attacker uncovers one session key, it may be useless to the attacker, in which case he now has to work to identify a new session key.
- So breaking an algorithm can take place through brute force attacks or by identifying weaknesses in the algorithm itself. Brute force attacks have increased in potency because of the increased processing capacity of computers today.
- An algorithm that uses a 40-bit key has around 1 trillion possible key values. If a 56-bit key is used, then there are approximately 72 quadrillion different key values. Relative to today's computing power, these key sizes do not provide much protection at all.

15. If you are supposed to implement one-time pad encryption scheme, which requirements do you think, each pad fulfill so that it is unbreakable?

For a one-time pad encryption scheme to be considered unbreakable, each pad in the scheme must be:

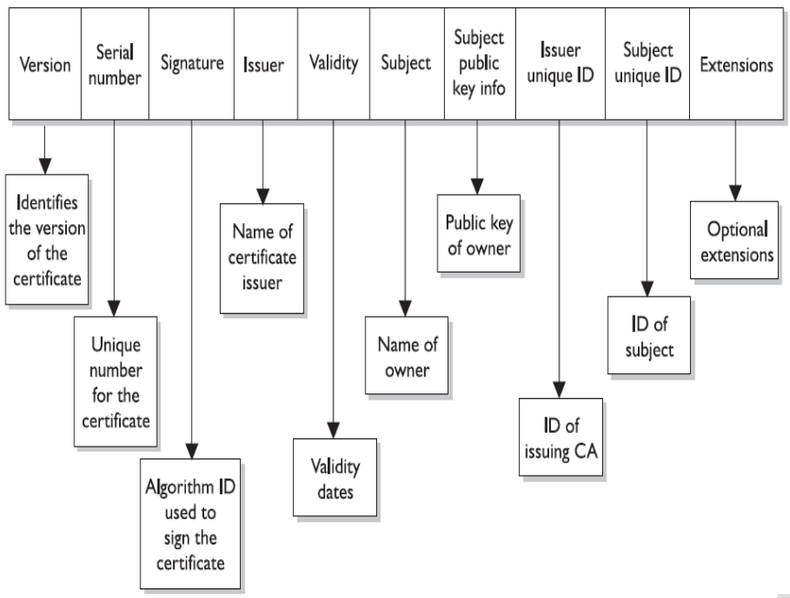
- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender's and receiver's sites
- At least as long as the message

A number generator is used to create a stream of random values and must be seeded by an initial value. This piece of software obtains its seeding value from some component within the computer system (time, CPU cycles, and so on). Although a computer system is complex, it is a predictable environment, so if the seeding value is predictable in any way, the resulting values created are not truly random—but pseudorandom.

16. List and briefly describe the parts of digital certificates

- Serial number
- Version number
- Identity information
- Algorithm information
- Lifetime dates

Signature of the issuing authority etc as shown in the Figure.



17. What are payloads? How they can be harmful? Explain with the help of an example.

a. Pieces of code that do damage
b. Implemented by viruses and worms after propagation
c. Malicious payloads are designed to do heavy damage

1. Benign payloads merely pop up a message on the user's screen or do some other annoying but nonlethal damage
2. Malicious payloads can do extreme damage, for example, by randomly deleting files from the victim's hard disk drive or by installing some other types of malware
3. Virus and worm payloads also frequently soften up the computer by disabling its antivirus software and by taking other actions that leave it highly vulnerable to subsequent virus and worm attacks

Example:

In 2004, the Aberdeen group surveyed 162 companies. They found that each firm lost an average of USD 2 million per virus or worm incident and spent an additional USD 100,000 to clean up computers after an attack. Both numbers increased with company size. Most companies reported enduring on average one incident per year, although many firms reported multiple incidents. (http://www.aberdeen.com)

18. Why is the middle portion of 3DES a decryption rather than an encryption?

3DES Modes

DES-EEE3 Uses three different keys for encryption, and the data are encrypted, encrypted, encrypted

DES-EDE3 Uses three different keys for encryption, and the data are encrypted, decrypted, and encrypted

DES-EEE2 The same as DES-EEE3 but uses only two keys, and the first and third encryption processes use the same key

DES-EDE2 The same as DES-EDE3 but uses only two keys, and the first and third encryption processes use the same key

EDE (Middle Portion) ?

EDE may seem a little odd at first. How much protection could be provided by encrypting something, decrypting it, and encrypting it again? The decrypting portion here is decrypted with a different key. When data are encrypted with one symmetric key and decrypted with a different symmetric key, it is jumbled(misordered) even more. So the data are not actually decrypted in the middle function, they are just run through a decryption process with a different key.

19. Enlist three approaches to message authentication.

1. Message Authentication Using Conventional Encryption

   Only the sender and receiver should share a key

2. Message Authentication without Message Encryption

   An authentication tag is generated and appended to each message

3. Message Authentication Code

   Calculate the MAC as a function of the message and the key. MAC = F(K, M)

20. How is an X.509 certificate revoked?

Unsolved…

21. PKI Security Services

PKI supplies the following security services:

- Confidentiality
- Access control
- Integrity
- Authentication
- Nonrepudiation

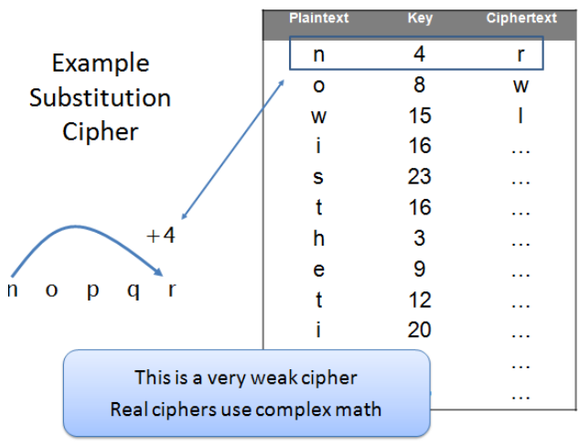
22. What are the two basic types of symmetric encryption? Elaborate each with the help of example.

Symmetric encryption ciphers come in two basic types:

- Substitution
- Transposition

Substitution cipher

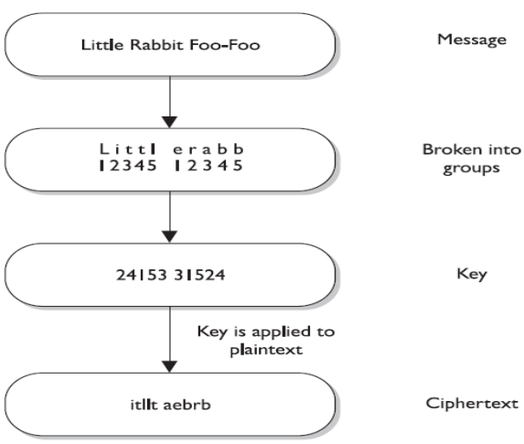
- The **substitution cipher** replaces bits, characters, or blocks of characters with different bits, characters, or blocks



- A substitution cipher uses a key to dictate how the substitution should be carried out
- In the **Caesar cipher,** each letter is replaced with the letter three places beyond it in the alphabet. The algorithm is the alphabet, and the key is the instruction "shift up three."
- Substitution is used in today's symmetric algorithms, but it is extremely complex compared to this example

Transposition Ciphers

- In a transposition cipher, the values are scrambled, or put into a different order
- The key determines the positions the values are moved to, as illustrated in the Figure
- This is a simplistic example of a transposition cipher and only shows one way of performing transposition
- When implemented with complex mathematical functions, transpositions can become quite sophisticated and difficult to break



23. What are the attributes that make the symmetric cryptography so powerful? Also give the limitations while using the symmetric key cryptography. 10

Symmetric Cryptography

- In a cryptosystem that uses symmetric cryptography, the sender and receiver use two instances of the same key for encryption and decryption, as shown in the Figure
- So the key has dual functionality, in that it can carry out both encryption and decryption processes

Attributes that make it so Powerful

- Much faster (less computationally intensive) than asymmetric systems
- Hard to break if using a large key size
- It is relatively inexpensive to produce a strong key for these ciphers.
- The keys tend to be much smaller for the level of protection they afford.
- The algorithms are relatively inexpensive to process

Therefore, implementing symmetric cryptography (particularly with hardware) can be highly effective because you do not experience any significant time delay as a result of the encryption and decryption. Symmetric cryptography also provides a degree of authentication because data encrypted with one symmetric key cannot be decrypted with any other symmetric key. Therefore, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Limitations

- Secure key distribution
- Scalability
- Security services

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.
- Provides confidentiality but not authenticity or non repudiation
- Cannot provide digital signatures that cannot be repudiated.

24. In the context of Kerberos, Explain the concept of realm?

- A Kerberos realm is a set of managed nodes that share the same Kerberos database. The Kerberos database resides on the Kerberos master computer system, which should be kept in a physically secure room. A read-only copy of the Kerberos database might also reside on other Kerberos computer systems. However, all changes to the database must be made on the master computer system. Changing or accessing the contents of a Kerberos database requires the Kerberos master password.
- A Kerberos principal is a service or user that is known to the Kerberos system. Each Kerberos principal is identified by its principal name. Principal names consist of three parts: a service or user name, an instance name, and a realm name in the following form:
- For example, a principal name could describe the authorization role the user has in a particular realm, such as joe.user@realm1 for a user principal. A principal name can also describe the location of a service on a computer system, for example, ftp.host1@realm2 for a service principal. The instance part of the principal name is optional but is useful for identifying the computer system on which a service resides. Kerberos considers identical services on different computer systems to be different service principals.
- Each principal has a principal password, which Kerberos uses during its authentication process to authenticate services and users to each other. With Kerberos, a principal on one computer system in a network can talk to a principal on another computer system in the network with confidence, knowing that the service or user is what or who it says it is.
- For each computer system that is part of the Kerberos realm, the **ext_srvtab** command creates the srvtab file in the /etc directory. This file contains information that relates to service or user principals that have an instance on the computer system. If no service or user principals are on a computer system, the srvtab file is empty.
- When a user logs in as a Kerberos principal, Kerberos assigns the user a ticket. Each ticket has a lifetime, which determines the length of time for which the ticket is valid. When a ticket expires, the principal is no longer

trusted and is unable to perform additional work until a new ticket has been acquired.

Creating a Kerberos Realm

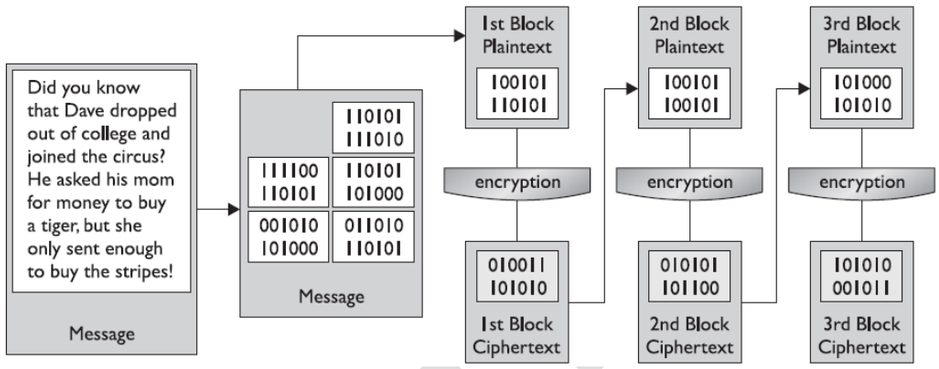
- Select a computer system to serve as the master of the realm
- Ensure that Kerberos commands are in your search path
- Create a Kerberos configuration file
- Initialize and populate the distribution center key database on the master
- Create one or more Tivoli administrators as Kerberos principals
- Set up any other computer systems in the realm
- Ensure that the Tivoli daemon is configured to use Kerberos authentication

25. What is CMAC. Define its functionality.

CMAC is a block cipher–based message authentication code algorithm. This means that it can provide the authentication of the data origin (as in the computer it was sent from) but not the person who sent it.

CMAC Functionality

So here is how CMAC works: the symmetric algorithm (AES or 3DES) creates the symmetric key. This key is used to create subkeys. The subkeys are used individually to encrypt the individual blocks of a message as shown in the Figure.



This is the exactly how CBC-MAC works, but with some better magic that works underneath the hood.

26. Differentiate between private and secret key.

- **Secret key** is used in symmetric cryptography where only one key is needed for encryption and decryption
- **Private and public key** are the two keys that two different entities are using in public key cryptography to decrypt (using the private) what have been encrypted with the public or reverse.

27. What are main components of Kerberos?

When using the Kerberos protocol , a Key Distribution Center (KDC) is used to store, distribute, and maintain cryptographic session and secret keys.

Kerberos Software Components

The Athena implementation comprises several modules:

- Kerberos applications library
- encryption library
- database library
- database administration programs
- administration server
- authentication server
- db propagation software
- user programs
- applications

28. What is an asymmetric key algorithm?

Symmetric vs. asymmetric algorithms:

When using **symmetric algorithms**, both parties share the same key for en- and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe any more. Symmetric algorithms have the advantage of not consuming too much computing power. A few well-known examples are: DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, TWOFISH.

Asymmetric algorithms use pairs of keys. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called ``private key'' or ``secret key'', while the encryption key is spread to all who

encrypted messages to the owner of the secret key. The secret key can't be reconstructed from the public key. The idea of asymmetric algorithms was first published 1976 by Diffie and Hellmann.

29. Strengths & Weaknesses of Asymmetric Encryption

Strengths

- Better key distribution than symmetric systems
- Better scalability than symmetric systems
- Can provide authentication and nonrepudiation

Weaknesses

- Works much more slowly than symmetric systems
- Mathematically intensive tasks

30. What are the main components of symmetric encryptions? Describe its limitations.

(unsolved)

31. What is ECC algorithm.

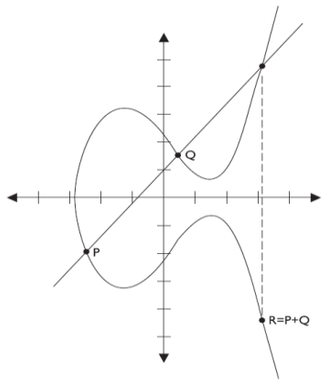
An elliptic curve cryptosystem (ECC) provides much of the same functionality RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency.

Eliptic Curves

In this field of mathematics, points on the curves compose a structu

Elliptic Curve Cryptosystems

The Figure is an example of an elliptic curve. In this field of mathematics, points on the curves compose a structure called a group. These points are the values used in mathematical formulas for ECC's encryption and decryption processes.



T hic ogarithms in a finite field (which is what Diffie-Hellman and El Gamal use).

- Some devices have limited processing capacity, stora h as wireless devices and cellular telephones. With these types of device rtant.
- ECC provides encryption functionality,requiring a smaller percentage of the resources needed by RSA and other algorithms, so it is used in these types of devices.
- In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter than what RSA requires.
- Because longer keys require more resources to perform mathematical tasks, the smaller keys used in ECC require fewer resources of the device.

32. What are the categories of security services? Briefly explain them. 5 marks

PKI supplies the following security services:

- Confidentiality
- Access control
- Integrity
- Authentication
- Nonrepudiation

A PKI must retain a key history, which keeps track of all the old and current public keys that have been used by individual users. For example, if Kevin encrypted a symmetric key with Dave's old public key, there should be a way for Dave to still access this data. This can only happen if the CA keeps a proper history of Dave's old certificates and keys.

33. Briefly describe the features of the Advanced Encryption Algorithm (Rijndael). [5]

The block sizes that Rijndael supports are 128, 192, and 256 bits. The number of rounds depends upon the size of the block and the key length:

- If both the key and block size are 128 bits, there are 10 rounds
- If both the key and block size are 192 bits, there are 12 rounds
- If both the key and block size are 256 bits, there are 14 rounds

Rijndael works well when implemented in software and hardware in a wide range of products and environments. It has low memory requirements and has been constructed to easily defend against timing attacks.

Rijndael was NIST's choice to replace DES. It is now the algorithm required to protect sensitive but unclassified

34. List and briefly describe the fields that are part of a digital certificate. [10]

- **Version number:** Version number of the X.509 standard. Most certificates follow Version 3. Different versions have different fields.
- **Issuer:** Name of the certificate authority (CA).
- **Serial Number**: Unique serial number for the certificate, set by the CA.
- **Subject:** The name of the person, organization, computer, or program to which the certificate has been issued. This is the true party.
- **Public Key:** The public key of the subject (the true party).
- **Public Key Algorithm:** The algorithm the subject uses to sign messages with digital signatures
- **Valid Period:.** The period before which and after which the certificate should not be used. Note: Certificate may be revoked before the end of this period.
- **Digital Signature**: The digital signature of the certificate, signed by the CA with the CA's own private key. For testing certificate authentication and integrity. User must know the CA's public key independently.
- **Signature Algorithm Identifier:** The digital signature algorithm the CA uses to sign its certificates.
- **Other Fields:**

35. If you are supposed to implement one-time pad encryption scheme, which requirements do you think, each pad fulfill so that it is unbreakable?

A one-time pad is a perfect encryption scheme because it is considered unbreakable if implemented properly.
For a one-time pad encryption scheme to be considered unbreakable, each pad in the scheme must be:

- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender's and receiver's sites
- At least as long as the message

36. Differentiate between public key cryptography and public key infrastructure.

- These algorithms are used to create public/private key pairs, perform key exchange or agreement, and generate and verify digital signatures. Note that public key cryptography can only perform key agreement and cannot generate or verify digital signatures.
- Public key infrastructure (PKI) is different. It is not an algorithm, a protocol, or an application. It is an infrastructure based on public key cryptography.

37. What are the two basic functions used in encryption algorithms?

All the encryption Algorithms are based on two general Principles:

- **Substitution:** In which each element in the plaintext (bit, letter , group, of bits or letters is mapped into another element.
- **Transposition:** In which elements in the plaintext are arranges. The fundamentals requirements is that no information be lost (that is, that all operations are reversible). Most system referred to as product systems, involve multiple stages of substitution and transposition.

38. Differentiate between Kerberos version 4 and version 5. [5]

	Kerberos Version 4	**Kerberos Version 5**
Chronology	Kerberos v4 was released prior to the version 5 in the late 1980's.	The version 5 was published in 1993, years after the appearance of version 5.
Key salt algorithm	Uses the principal name partially.	Uses the entire principal name.
Encoding	Uses the "receiver-makes-right" encoding system.	Uses the ASN.1 coding system.
Ticket support	Satisfactory	Well extended. Facilitates forwarding, renewing and postdating tickets.
Transitive cross-realm authentication support	No present support for the cause.	Reasonable support present for such authentication.

39. How AES encryption works?

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

40. You are appointed as a network security personnel in an organization, if u are using the symmetric key encryption, what will be yours arguments in favour and against the use of this algorithm? 5 marks

Unsolved

41. Consider A 32-bit has function implemented as two 16-bit functions using XOR and RXOR. Is created checksum by concatenation the both detects all the odd parity errors? Explain. If these functions are used for authentication what will be the effectiveness of the authentication.

Consider a 32-bit hash function defined as the concatenation of two 16-bit functions: XOR and RXOR, which are defined in Section 3.2 as “two simple hash functions.”

a) Will this checksum detect all errors caused by an odd number of error bits? Explain.
b) Will this checksum detect all errors caused by an even number of error bits? If not, characterize the error patterns that will cause the checksum to fail.
c) Comment on the effectiveness of this function for use as a hash function for authentication.

Solution:

a) Yes. The XOR function is simply a vertical parity check. If there is an odd number of errors, then there must be at least one column that contains an odd number of errors, and the parity bit for that column will detect the error. Note that the RXOR function also catches all errors caused by an odd number of error bits. Each RXOR bit is a function of a unique “spiral” of bits in the block of data. If there is an odd number of errors, then there must be at least one spiral that contains an odd number of errors, and the parity bit for that spiral will detect the error.
b) No. The checksum will fail to detect an even number of errors when both the XOR and RXOR functions fail. In order for both to fail, the pattern of error bits must be at intersection points between parity spirals and parity columns such that there is an even number of error bits in each parity column and even number of error bits in each spiral.
c) It is too simple to be used as a secure hash function; finding multiple message with the same hash function would be too easy.