Cryptography

B.karthicsonia

Abstract-Cryptography operates by a sender scrambling or encrypting the original message or plaintext in a systematic way that obscures its meaning. The encrypted message or crypto text is transmitted, and the receiver recovers the message by unscrambling or decrypting the transmission.”“Cryptography” referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called cipher text). Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text. “Cryptanalysis” is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations.

Index Terms: History of cryptography, Classic cryptographic techniques, Modern cryptographic techniques: PUBLIC KEY ENCRYPTION(Asymmetric-key cryptography),Public key infrastructure, Digital signature

INTRODUCTION:

Cryptography operates by a sender scrambling or encrypting the original message or plaintext in a systematic way that obscures its meaning. The encrypted message or crypto text is transmitted, and the receiver recovers the message by unscrambling or decrypting the transmission.”“Cryptography” referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called cipher text). Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text. “Cryptanalysis” is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations.

History of cryptography:

Cryptography was concerned solely with message confidentiality (i.e., encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message).

Encryption was used

- **To ensure secrecy in communications**
- **Message integrity checking**
- **Sender/receiver identity authentication**
- **Digital signatures**
- **Interactive proofs and secure computations.**

Classic cryptographic techniques:

Existing cryptographic techniques are usually identified as "Traditional" or "Modern."

Traditional cryptographic techniques :

Use operations of coding(ie)use of alternative words or phrase.

The main classical cipher types are:

1.Transposition ciphers

2.Substitution Ciphers

1.Transposition ciphers:

Rearrange the order of letters in a message ,e.g., 'cryptography' becomes 'rctypotrgpayh' in a trivially simple rearrangement scheme.

2.Substitution Ciphers:

Replace letters or groups of letters with other letters or groups of letters ,e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet.

Modern cryptographic techniques:

There are two Branches of modern cryptographic techniques:

1.SECRET KEY ENCRYPTION.

2.PUBLIC KEY ENCRYPTION

SECRET KEY ENCRYPTION (Symmetric-key cryptography)

In secret key encryption, a k-bit "secret key" is shared by two users, who use it to transform plaintext inputs to cryptotext for transmission and back to plaintext upon receipt. To make unauthorized decipherment more difficult, the transformation algorithm can be carefully designed to make each bit of output depend on every bit of the input. With such an arrangement, a key of 128 bits used for encoding results in a choice of about 1038 numbers. The encrypted message should be secure; assuming that brute force and massive parallelism are employed, a billion computers doing a billion operations per second would require a trillion years to decrypt it. In practice, analysis of the encryption algorithm might make it more vulnerable, but increases in the size of the key can be used to offset this.

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government. Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access.

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher.

Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input, and output a short, fixed length hash which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function which is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt.

The main practical problem with secret key encryption is exchanging a secret key. In principle any two users who wished to communicate could first meet to agree on a key in advance, but in practice this could be inconvenient. Other methods for establishing a key, such as the use of secure courier or private knowledge, could be impractical for routine communication between many users. But any discussion of how the key is to be chosen that takes place on a public communication channel could in principle be intercepted and used by an eavesdropper.

One proposed method for solving this key distribution problem is the appointment of a central key distribution server. Every potential communicating party registers with the server and establishes a secret key. The server then relays secure communications between users, but the server itself is vulnerable to attack. Another method is a protocol for agreeing on a secret key based on publicly exchanged large prime numbers, as in the Diffie Hellman key exchange. Its security is based on the assumed difficulty of finding the power of a base that will generate a specified remainder when divided by a very large prime number, but this suffers from the uncertainty that such problems will remain intractable. Quantum encryption, which will be discussed later, provides a way of agreeing on a secret key without making this assumption.

PUBLIC KEY ENCRYPTION(Asymmetric-key cryptography):

In public key encryption, Each participant has a "public key" and a "private key"; the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them.

The widely used RSA algorithm is one example of public key cryptosystem Anyone wanting to receive a message publishes a key, which contains two numbers. A sender converts a message into a series of digits, and performs a simple mathematical calculation on the series using the publicly available numbers. Messages are deciphered by the recipient by performing another operation, known only to him . In principle, an eavesdropper could deduce the decryption method by factoring one of the published numbers, but this is chosen to typically exceed 100 digits and to be the product of only two large prime numbers, so that there is no known way to accomplish this factorization in a practical time.

The nicest example of public key cryptosystem (and undoubtedly the simplest) was presented two years later in 1978. It was invented by Rivest, Shamir and Adleman and is therefore shortened RSA. It is based on the mathematical difficulty of integer factorization. The private key is made out of the triplet (p,q,d) with p and q two primes (having roughly same size), and d a relative prime to p-1 and q-1. The public key is made of pair (n,e), with n=pq, and e the inverse of d modulus (p-1)(q-1),i.e.

$$ed = 1 \mod (p-1)(q-1).$$

Suppose Alice wants to send some text, enciphered with Bob's public key (n,e). She first transforms the message in an integer m less than n. Then, she processes

$$c = me \mod n,$$

and sends the result c over to Bob. On his side, Bob whose private key is (p,q,d) processes :

$$cd \mod n = med \mod n = m.$$

For RSA, the one-way trap function is the function which associates an integer x <n to the value xe mod n.

Since RSA, many other public key cryptosystems have been invented. Currently, one of the most famous alternatives to RSA is a cryptosystem based on discrete logarithms.

ADVANTAGE:

Public-key cryptography can also be used for implementing digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the content of the message being signed; they cannot then be 'moved' from one document to another, for any attempt will be detectable. In digital signature schemes, there are two algorithms: one for signing, in which a secret key is used to process the message (or a hash of the message, or both), and one forverification, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (e.g.,SSL/TLS, many VPNs, etc.).

DIS ADVANTAGE:

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie–Hellman and DSA are related to the discrete logarithm problem. elliptic curve cryptography has developed in which security is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems, in which a fast high-quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

Modern use of cryptography

Actually, public key cryptography is really interesting because it is easy to use and it solves many security problems heretofore unsolved. More precisely, it solves a few authentication problems:

- Identifying individuals: using anonymous communications means of today, Alice wants to be sure the person with whom she is talking is not cheating and impersonating Bob. To do so, she uses an identification protocol. Multiple identification protocols exist and commonly rely on the principles of RSA or of discrete logarithm.
- Document authentication: an authority authenticates documents through a digital signature. Signing consists in appending a few bits which are the result of some processing with document and authority as input, and which are generally hashed by a hash algorithm such as MD5 or SHA. Moreover, any person with access to the document should be able to verify that signature has really been issued by the authority. To do so, signature schemas are used. One of the most famous signature scheme is ElGamal - once more based on discrete logarithm problems.

Besides, as secret key cryptography, public key cryptography provides encryption-based cryptosystems, guaranteeing confidentiality of communications.

Let's imagine Alice wants to communicate secretly with Bob. Alice retrieves Bob's public key in a public directory, and enciphers her message with this key. When Bob receives the ciphertext, he uses his private key to decipher the ciphertext and read initial clear text. Both keys have very different roles, this explains why such systems are called asymmetric cryptosystems - referring to secret key cryptosystems which use the same key for ciphering and deciphering and are also know as symmetric cryptosystems.

Public key cryptography offers another major benefit over secret key cryptography:

If n users communicate through a secret key cryptosystem, each of them need one different secret key for each person in the group. So, n(n-1) keys need to be managed. If n is over thousands of users, then millions of keys need to be managed... Furthermore, adding a new user to the group is not an easy task, because n new keys need to be generated for the user to communicate with all members of the group. Then, those new keys need to be sent over to the group. On the contrary, in asymmetric cryptosystems, the n public keys of the members are stored in a public directory. Adding a new user simply consists in adding his public key to the directory.

Using a public or a secret key: finding a trade-off

The previous paragraph has explained that public key cryptography solved many problems secret key cryptography could not cope with. One might then wonder what for AES has been designed. Actually, there are two major explanations to this choice.

- First, a practical reason. Generally, public key cryptosystems are very slow. For instance, software implementations of RSA are a thousand times slower than AES, and RSA has not been designed with hardware implementation in mind. Transmitting information is so crucial today, we cannot accept to be limited by a cipher algorithm.
- Second, public key cryptosystems' inner structure lead to other security problems.

  For instance, public key cryptosystems require much larger key sizes - for a correct security level - than secret key cryptosystems. Actually, the notion and importance given to key length should only be considered in secret key cryptosystems. As a matter of fact, those systems rely on the fact that only brute-force attacks might defeat them, i.e. enumerating all possible keys. If key length is 128 bits, then 2128 should be enumerated.

  But with public key cryptosystems, key size is only an interesting parameter when considering the same system. For instance, RSA with a 512 bit key is less secure than AES with a 128 bit key. The only way to correctly evaluate a public key cryptosystem is to assess the complexity of the best known attack, and this is quite different: one never knows if a new invention is going to compromise the system's security. Recently, a group of researchers successfully factored a 512 bit integer. Consequently, for a correct security level, the usual advice is to use 1024 bit numbers.

As a consequence, for pure encipherment, secret key algorithms are preferred - when it's possible to use them. Zimmermann has worked over an interesting hybrid solution, implemented in PGP. Basically, when Alice and Bob want to communicate with integrity features, using a secret key algorithm (PGP uses IDEA):

- Alice and Bob negotiate a secret key using a key exchange protocol. Key exchange protocols use public key cryptography. One of the most famous protocols relies on Diffie-Hellman's algorithm.
- Then, they communicate using the IDEA algorithm.

When they have finished communicating, the negotiated session key is discarded. Such a system uses both secret key cryptosystems and public key cryptosystems. Usually, people consider the less secure part of such a system is the key exchange protocol.

Public key infrastructure

Public Key Infrastructure (PKI) is a framework that enables integration of various services that are related to cryptography.

The aim of PKI is to provide confidentiality, integrity, access control, authentication, and most importantly, non-repudiation.

> Non-repudiation is a concept, or a way, to ensure that the sender or receiver of a message cannot deny either sending or receiving such a message in future. One of the important audit checks for non-repudiation is a time stamp. The time stamp is an audit trail that provides information of the time the message is sent by the sender and the time the message is received by the receiver.

Encryption and decryption, digital signature, and key exchange are the three primary functions of a PKI.

RSS and elliptic curve algorithms provide all of the three primary functions: encryption and decryption, digital signatures, and key exchanges. Diffie-Hellmen algorithm supports key exchanges, while Digital Signature Standard (DSS) is used in digital signatures.

Public Key Encryption is the encryption methodology used in PKI and was initially proposed by Diffie and Hellman in 1976. The algorithm is based on mathematical functions and uses asymmetric cryptography, that is, uses a pair of keys.

The image above represents a simple document-signing function. In PKI, every user will have two keys known as "pair of keys". One key is known as a private key and the other is known as a public key. The private key is never revealed and is kept with the owner, and the public key is accessible by every one and is stored in a key repository.

A key can be used to encrypt as well as to decrypt a message. Most importantly, a message that is encrypted with a private key can only be decrypted with a corresponding public key. Similarly, a message that is encrypted with a public key can only be decrypted with the corresponding private key.

In the example image above, Bob wants to send a confidential document to Alice electronically. Bob has four issues to address before this electronic transmission can occur:

1. Ensuring the contents of the document are encrypted such that the document is kept confidential.
2. Ensuring the document is not altered during transmission.
3. Since Alice does not know Bob, he has to somehow prove that the document is indeed sent by him.
4. Ensuring Alice receives the document and that she cannot deny receiving it in future.

PKI supports all the above four requirements with methods such as secure messaging, message digests, digital signatures, and non-repudiation services.

Secure messaging

To ensure that the document is protected from eavesdropping and not altered during the transmission, Bob will first encrypt the document using Alice's public key. This ensures two things: one, that the document is encrypted, and two, only Alice can open it as the document requires the private key of Alice to open it. To summarize, encryption is accomplished using the public key of the receiver and the receiver decrypts with his or her private key. In this method, Bob could ensure that the document is encrypted and only the intended receiver (Alice) can open it. However, Bob cannot ensure whether the contents are altered (Integrity) during transmission by document encryption alone.

Message digest

In order to ensure that the document is not altered during transmission, Bob performs a hash function on the document. The hash value is a computational value based on the contents of the document. This hash value is known as the message digest. By performing the same hash function on the decrypted document the message, the digest can be obtained by Alice and she can compare it with the one sent by Bob to ensure that the contents are not altered.

This process will ensure the integrity requirement.

Digital signature

In order to prove that the document is sent by Bob to Alice, Bob needs to use a digital signature. Using adigital signature means applying the sender's private key to the message, or document, or to the message digest. This process is known as as signing. Only by using the sender's public key can the message be decrypted.

Bob will encrypt the message digest with his private key to create a digital signature. In the scenario illustrated in the image above, Bob will encrypt the document using Alice's public key and sign it using his digital signature. This ensures that Alice can verify that the document is sent by Bob, by verifying the digital signature (Bob's private key) using Bob's public key. Remember a private key and the corresponding public key are linked, albeit mathematically. Alice can also verify that the document is not altered by validating the message digest, and also can open the encrypted document using her private key.

> Message authentication is an authenticity verification procedure that facilitates the verification of the integrity of the message as well as the authenticity of the source from which the message is received.

Digital certificate

By digitally signing the document, Bob has assured that the document is sent by him to Alice. However, he has not yet proved that he is Bob. To prove this, Bob needs to use a digital certificate.

A digital certificate is an electronic identity issued to a person, system, or an organization by a competent authority after verifying the credentials of the entity. A digital certificate is a public key that is unique for each entity. A certification authority issues digital certificates.

In PKI, digital certificates are used for authenticity verification of an entity. An entity can be an individual, system, or an organization.

An organization that is involved in issuing, distributing, and revoking digital certificates is known as aCertification Authority (CA). A CA acts as a notary by verifying an entity's identity.

One of the important PKI standards pertaining to digital certificates is X.509. It is a standard published by the International Telecommunication Union (ITU) that specifies the standard format for digital certificates.

PKI also provides key exchange functionality that facilitates the secure exchange of public keys such that the authenticity of the parties can be verified.

Key management procedures

Key management consists of four essential procedures concerning public and private keys. They are as follows:

1. Secure generation of keys—Ensures that private and public keys are generated in a secure manner.
2. Secure storage of keys—Ensures that keys are stored securely.
3. Secure distribution of keys—Ensures that keys are not lost or modified during distribution.
4. Secure destruction of keys—Ensures that keys are destroyed completely once the useful life of the key is over.

Type of keys

NIST Special Publication 800-57 titled Recommendation for Key Management - Part 1: General specifies the following nineteen types of keys:

1. Private signature key—It is a private key of public key pairs and is used to generate digital signatures. It is also used to provide authentication, integrity, and non-repudiation.

2. Public signature verification key—It is the public key of the asymmetric (public) key pair. It is used to verify the digital signature.
3. Symmetric authentication key—It is used with symmetric key algorithms to provide assurance of the integrity and source of the messages.
4. Private authentication key—It is the private key of the asymmetric (public) key pair. It is used to provide assurance of the integrity of information.
5. Public authentication key—Public key of an asymmetric (public) pair that is used to determine the integrity of information and to authenticate the identity of entities.
6. Symmetric data encryption key—It is used to apply confidentiality protection to information.
7. Symmetric key wrapping key—It is a key-encryptin key that is used to encrypt the other symmetric keys.
8. Symmetric and asymmetric random number generation keys—They are used to generate random numbers.
9. Symmetric master key—It is a master key that is used to derive other symmetric keys.
10. Private key transport key—They are the private keys of asymmetric (public) key pairs, which are used to decrypt keys that have been encrypted with the associated public key.
11. Public key transport key—They are the public keys of asymmetric (public) key pairs that are used to decrypt keys that have been encrypted with the associated public key.
12. Symmetric agreement key—It is used to establish keys such as key wrapping keys and data encryption keys using a symmetric key agreement algorithm.
13. Private static key agreement key—It is a private key of asymmetric (public) key pairs that is used to establish keys such as key wrapping keys and data encryption keys.
14. Public static key agreement key— It is a public key of asymmetric (public) key pairs that is used to establish keys such as key wrapping keys and data encryption keys.
15. Private ephemeral key agreement key—It is a private key of asymmetric (public) key pairs used only once to establish one or more keys such as key wrapping keys and data encryption keys.
16. Public ephemeral key agreement key—It is a public key of asymmetric (public) key pairs that is used in a single key establishment transaction to establish one or more keys.
17. Symmetric authorization key—This key is used to provide privileges to an entity using symmetric cryptographic method.
18. Private authorization key—It is a private key of an asymmetric (public) key pair that is used to provide privileges to an entity.
19. Public authorization key—It is a public key of an asymmetric (public) key pair that is used to verify privileges for an entity that knows the associated private authorization key.

Key management best practices

Key Usage refers to using a key for a cryptographic process, and should be limited to using a single key for only one cryptographic process. This is to ensure that the strength of the security provided by the key is not weakened.

When a specific key is authorized for use by legitimate entities for a period of time, or the effect of a specific key for a given system is for a specific period, then the time span is known as a cryptoperiod. The purpose of defining a cryptoperiod is to limit a successful cryptanalysis by a malicious entity.

> Cryptanalysis is the science of analyzing and deciphering code and ciphers.

The following assurance requirements are part of the key management process:

- Integrity protection—Assuring the source and format of the keying material by verification
- Domain parameter validity—Assuring parameters used by some public key algorithms during the generation of key pairs and digital signatures, and the generation of shared secrets that are subsequently used to derive keying material
- Public key validity—Assuring that the public key is arithmetically correct
- Private key possession—Assuring that the possession of the private key is obtained before using the public key

Cryptographic algorithm and key size selection are the two important key management parameters that provide adequate protection to the system and the data throughout their expected lifetime.

Key states

A cryptographic key goes through different states from its generation to destruction. These states are defined as key states. The movement of a cryptographic key from one state to another is known as a key transition.

NIST SP800-57 defines the following six key states:

- Pre-activation state—The key has been generated, but not yet authorized for use
- Active state—The key may used to cryptographically protect information
- Deactivated state—The cryptoperiod of the key is expired, but the key is still needed to perform cryptographic operations
- Destroyed state—The key is destroyed
- Compromised state—The key is released or determined by an unauthorized entity
- Destroyed compromised state—The key is destroyed after a compromise or the comprise is found after the key is destroyed

Key management phases

The key states, or transitions, can be grouped under four key management phases. They are as follows

- Pre-operational phase—The keying material is not yet available for normal cryptographic operations
- Operational phase—The keying material is available for normal cryptographic operations and is in use
- Post-operational phase—The keying material is no longer in use, but access to the material is possible
- Destroyed phase—The keys are no longer available

Methods of cryptanalytic attacks

Cryptanalytic attacks are keys that have been compromised by decipherment to find out the keys. The goal of cryptanalysis is to decipher the private key or secret key. The amount of information provided to the analyst, as well as the type of information provided, determines the type of attacks possible. The following are six possible attack scenarios. Candidates are advised to understand the key difference between the different types of attacks.

1. Ciphertext only attack: This type of attack refers to the availability of the ciphertext (encrypted text) to the cryptanalyst. With large ciphertext data, it may be possible to decipher the ciphertext by analyzing the pattern.
2. Known-plaintext attack: This type of attack happens when a cryptanalyst obtains a ciphertext as well as the corresponding plaintext. In this scenario, even if the data is small, it is possible to understand the algorithm.
3. Chosen-plaintext attack: This type of attack refers to the availability of a corresponding ciphertext to the block of plaintext chosen by the analyst.
4. Adaptive-chosen-plaintext attack: This type of cryptanalytic attack is known as an adaptive-chosen-plaintext attack if the cryptanalyst can choose the samples of the plaintext based on the results of previous encryptions in a dynamic passion.
5. Chosen-ciphertext attack: This type of attack is used to obtain the plaintext by choosing a sample of ciphertext by the cryptanalyst.
6. Adaptive-chosen-ciphertext attack: This type of attack is similar to the chosen-ciphertext attack, but the samples of ciphertext are dynamically selected by the cryptanalyst and the selection can be based on the previous results as well.

Cryptographic standards

Cryptography standards are related to the following:

- Encryption
- Hashing
- Digital signatures
- Public Key Infrastructure
- Wireless
- Federal standards

In this section of the article we'll cover the wireless standards and the Federal standard FIPS-140 for cryptographic modules.

Wireless cryptographic standards

Wireless protocols and services are predominantly governed by IEEE 802.11 standards. These standards are basically for Wireless Local Area Network (WLAN) computer communications.

The following are some of the cryptographic standards that are used in WLAN:

Wired Equivalent Privacy (WEP) is an algorithm that uses stream cipher RC4 encryption standard for confidentiality protection and CRC-32 for integrity assurance. This algorithm is now deprecated as it is easily breached.

Wi-Fi Protected Access (WPA) is a security protocol developed by the Wi-Fi alliance that replaces WEP. This protocol implements the majority of the advanced requirements in the IEEE802.11i standard released in 2004. WPA is backward compatible with WEP.

WPA2 is an advanced protocol certified by the Wi-Fi alliance. This protocol fulfills the mandatory requirements of the IEE 822.11i standard and uses the AES algorithm for encryption.

> IEEE 802.11 is a set of standards that govern wireless networking transmission methods. IEEE 802.11a, IEEE 802.11b, and 802.11g are different standards based on the throughput or bandwidth and the frequency band. IEEE 802.11i is an amendment to the original 802.11 standards.
>
> The Wi-Fi alliance is a non-profit organization that supports IEEE wireless standards. The following is information about the Wi-Fi alliance as published on their web site: "The Wi-Fi Alliance is a global, non-profit industry association of more than 300 member companies devoted to promoting the growth of (WLANs). With the aim of enhancing the user experience for wireless portable, mobile, and home entertainment devices, the Wi-Fi Alliance's testing and certification programs help ensure the interoperability of WLAN products based on the IEEE 802.11 specification."

Bluetooth is a wireless protocol for short-range communications for fixed or portable computers and mobile devices. It uses the 2.4GHz short-range radio frequency bandwidth for communication between mobile devices, computers, printers, GPS, and more. Bluetooth uses custom block ciphers for confidentiality and authentication.

Federal information processing standard

We'll cover one of the most important federal standards titled Security Requirements for Cryptographic Modules FIPS-140 series in the following section:

> As per the published information: The Federal Information Processing Standards Publication Series of the NIST is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235. These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunication systems in the Federal Government. The NIST, through its Computer Systems Laboratory, provides leadership, technical guidance, and coordination of Government efforts in the development of standards and guidelines in these areas.

The core structure of FIPS140 recommends four security levels for cryptographic modules that protect sensitive information in the federal systems. These systems include computer and telecommunication systems that include voice system as well. The levels are qualitative in the increasing order, Level 1 being the lowest and Level 4 the highest.

The following are brief descriptions of the FIPS140 levels:

1. FIPS140 Security Level 1—It is the basic or lowest level of security that prescribes basic security requirements for a cryptographic module, such as using at least one approved cryptographic algorithm. This level does not emphasize physical security.
2. FIPS140 Security Level 2—Tamper evidence mechanisms is a requirement in this level. This enhances the physical security of the device. Tamper-evident seals or coatings should be used to physically protect the device or storage that contains the cryptographic module. This level also emphasizes the implementation of role-based authentication as a minimum.
3. FIPS140 Security Level 3—The primary requirement is preventing an intruder from

gaining access to the cryptographic modules and the Critical Security Parameters (CSP) contained within. This level prescribes high probability of detection and response mechanisms for physical attacks. This level emphasizes identity-based authentication.

4. **FIPS140 Security Level 4—This is the highest level and the physical security mechanisms. A complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access is provided. This level requires a two-factor authentication. This level also requires the control of environmental conditions such as preventing damage to cryptographic modules due to temperature, heat, and voltage.**

REFERENCES:

V. V. IA̅shchenko (2002). "Cryptography: an introduction". AMS Bookstore. p.6. ISBN 0-8218-2986-6
^ James Gannon, Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century, Washington, D.C., Brassey's, 2001, ISBN 1-57488-367-4.
b Bruce Schneier, Applied Cryptography, 2nd edition, Wiley, 1996, ISBN 0-471-11709-9.
^ Becket, B (1988). Introduction to Cryptology. Blackwell Scientific Publications. ISBN 0-632-01836-4. OCLC 16832704. **Excellent coverage of many classical ciphers and cryptography concepts and of the "modern" DES and RSA systems.**
James Gannon, **Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century, Washington, D.C., Brassey's, 2001,** ISBN 1-57488-367-4.