Design of secure e-voting system over a network is indeed a very difficult task as all the requirements of the voting system have to be met. Failure to ensure even one of the specifications can lead to chinks and glitches that can be exploited by a middleman to forge or manipulate the intricate details. Subsequently, the result of the election is computed from the sum of the votes which is jointly decrypted by the authorities. A voting scheme must ensure that the voter can keep his vote private.

**1.2 MultipleEncryptions**

Multiple encryptions are the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. It is also known as cascade encryption, cascade ciphering, multiple encryption, and superdecipherment. Superencryption refers to the outer-level encryption of a multiple encryption.

**Independent keys**

Picking any two ciphers, if the key used is the same for both, the second cipher could possibly undo the first cipher, partly or entirely. This is true of ciphers where the decryption process is exactly the same as the encryption process—the second cipher would completely undo the first. If an attacker were to recover the key through crypt analysis of the first encryption layer, the attacker could possibly decrypt all the remaining layers, assuming the same key is used for all layers.To prevent that risk, one can use keys that are statistically independent for each layer (e.g. independent RNGs).

**The Importance of the First Layer of Protection**

With the exception of the one-time password, no cipher has been theoretically proven to be unbreakable. Furthermore, some recurring properties may be found in the ciphertexts generated by the first cipher. Since those ciphertexts are the plaintexts used by the second cipher, the second cipher may be rendered vulnerable to attacks based on known plaintext properties.

This is the case when the first layer is a program P that always adds the same string S of characters at the beginning (or end) of all ciphertexts (commonly known as a magic number). When found in a file, the string S allows an operating system to know that the program P has to be launched in order to decrypt the file. This string should be removed before adding a second layer.

To prevent this kind of attack, one can use the method provided by Bruce Schneier to generate a random pad of the same size of the plaintext, then XOR the plaintext with the pad, resulting in a first ciphertext. Encrypt the pad and the first ciphertext with a different cipher and a different key, resulting in 2 more ciphertexts. Concatenate the last 2 ciphertexts in order to build the final ciphertext. A cryptanalyst must break both ciphers to get any information. This will, however, have the drawback of making the ciphertext twice as long as the original plaintext.

Note, however, that a weak first cipher may merely make a second cipher that is vulnerable to a chosen plaintext attack also vulnerable to a known plaintext attack. However, a block cipher must not be vulnerable to a chosen plaintext attack to be considered secure. Therefore, the second cipher described above is not secure under that definition, either. Consequently, both ciphers still need to be broken. The attack illustrates why strong assumptions are made about secure block ciphers and ciphers that are even partially broken should never be used.

**Digital Signature**

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

**Explanation**

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, [1] but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil,[4] and members of the European Union, electronic signatures have legal significance.

Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a nonsecure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals.[5] Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

**Definition**

Public-key cryptography

A digital signature scheme typically consists of three algorithms:

* A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
* A signing algorithm that, given a message and a private key, produces a signature.
* A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that act as a signature. It is formed by taking the hash of message and encrypting the message with creator's private key.

**Notions of Security**

In the foundational papers, Goldwasser, Micali, and Rivest lay out a hierarchy of attack models against digital signatures:

* In a key-only attack, the attacker is only given the public verification key.
* In a known message attack, the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker.
* In an adaptive chosen message attack, the attacker first learns signatures on arbitrary messages of the attacker's choice.
* They also describe a hierarchy of attack results:
* A total break results in the recovery of the signing key.
* A universal forgery attack results in the ability to forge signatures for any message.
* A selective forgery attack results in a signature on a message of the adversary's choice.
* An existential forgery merely results in some valid message/signature pair not already known to the adversary.
* The strongest notion of security, therefore, is security against existential forgery under an adaptive chosen message attack.

**Applications of Digital Signatures**

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory.

The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures.

Common reasons for applying a digital signature to communications:

**Authentication**

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

**Integrity**

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

**Non-Repudiation**

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentications, non-repudiation etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol".

Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.