CHAPTER 3

SYSTEM ANALYSIS & PLANNING

Systems analysis and design refers to the process of examining a business situation with the intent of improving it through better procedures and methods. Systems development can generally be thought of as having two major components: Systems Analysis and Systems Design. Systems design is the process of planning a new system or replace or complement an existing system. But before this planning can be done, we must thoroughly understand the existing system and determine how computers can best be used to make its operation more effective. Systems analysis, then, is the process of gathering and interpreting facts, diagnosing problems and using the information to recommend improvement to the system.

3.0 ANALYSIS OF THE EXISTING SYSTEM

In this paper review described techniques of cryptography are analyzed based on different research paper in respective journals

1. RSA (Rivest Shamir and Adleman) Algorithm

The Rivest-Shamir-Adleman (RSA) encryption algorithm is an asymmetric encryption algorithm that is widely used in many products and services. Asymmetric encryption uses a key pair that is mathematically linked to encrypt and decrypt data. A private and public key are created, with the public key being accessible to anyone and the private key being a secret known only by the key pair creator. With RSA, either the private or public key can encrypt the data, while the other key decrypts it. This is one of the reasons RSA is the most used asymmetric encryption algorithm.

The RSA algorithm involves three steps

1.1 Key generations

1.2 Encryption

1.3 Decryption

1.1 Key generation:

RSA involves a public key.The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

- Choose two distinct prime numbers p and q
- For security purposes, the integers p and q should be chosen at random
- Compute n = pq, where n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are coprime. e is released as the public key exponent.
- Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$). This is more clearly stated as solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$, where d is kept as the private key exponent.

- By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d

1.2 Encryption

Theresa transmits her public key (n,e) to Eben and keep the private key secret. Eben wishes to send message M to Theresa. He then computes the cipher text c corresponding to Eben and then transmits c to Theresa

1.3 Decryption

Theresa can recover m from c by using her private key exponent d via computing given m, she can recover the original message M by reversing the padding scheme

2. Digital Signature Algorithm(DSA)

It is used by the receiver of the message to verify that the message has not been altered during transmit as well as certain the sender's identity. A digital signature is an electronic version of a written signature in that the digital signature can be used in providing to the recipient or third party that the message was, in fact, signed by the sender. Digital signatures may also be generated for stored data and programs so that the integrity of the programs may be verify at any later time. One method for sending low size and capacity data by using DSA is proposed by Erfaneh Noorouzil et al. "Hash function" is used in this method and it generates dynamic and smaller size of bits which depends on each byte of data.

The main function which is used for hashing is bitwise or and multiply functions. If hashed file sized is 4% of the original file in the messages with size lower than 1600 bytes.

3.1 PROBLEMS OF THE EXISTING SYSTEM

1.RSA

The RSA algorithm raises a *message* to an exponent, modulo a composite number N whose factors are not known. Thus, the task can be neatly described as finding the e^{th} roots of an arbitrary number, modulo N. For large RSA key sizes (in excess of 1024 bits), no efficient method for solving this problem is known; if an efficient method is ever developed, it would threaten the current or eventual security of RSA-based cryptosystems—both for public-key encryption and digital signatures.

More specifically, the RSA problem is to efficiently compute P given an RSA public key (N, e) and a ciphertext $C \equiv P^e \pmod{N}$. The structure of the RSA public key requires that N be a large semiprime (i.e., a product of two large prime numbers), that $2 < e < N$, that e be coprime to $\varphi(N)$, and that $0 \leq C < N$. C is chosen randomly within that range; to specify the problem with complete precision, one must also specify how N and e are generated, which will depend on the precise means of RSA random keypair generation in use.

2.**Digital Signature Algorithm(DSA)**

- **Computational Basis of DSA Security**

The security of DSA is based on the computational difficulty in solving the discrete logarithm problem in prime fields and its subgroups, and it can be proved under the random oracle model [3], which assumes that the hash function behaves like a random oracle, i.e. its values are independent and uniformly distributed. It is cautioned in the standard that if the nonce (k) is disclosed, the secret-key can be easily recovered.

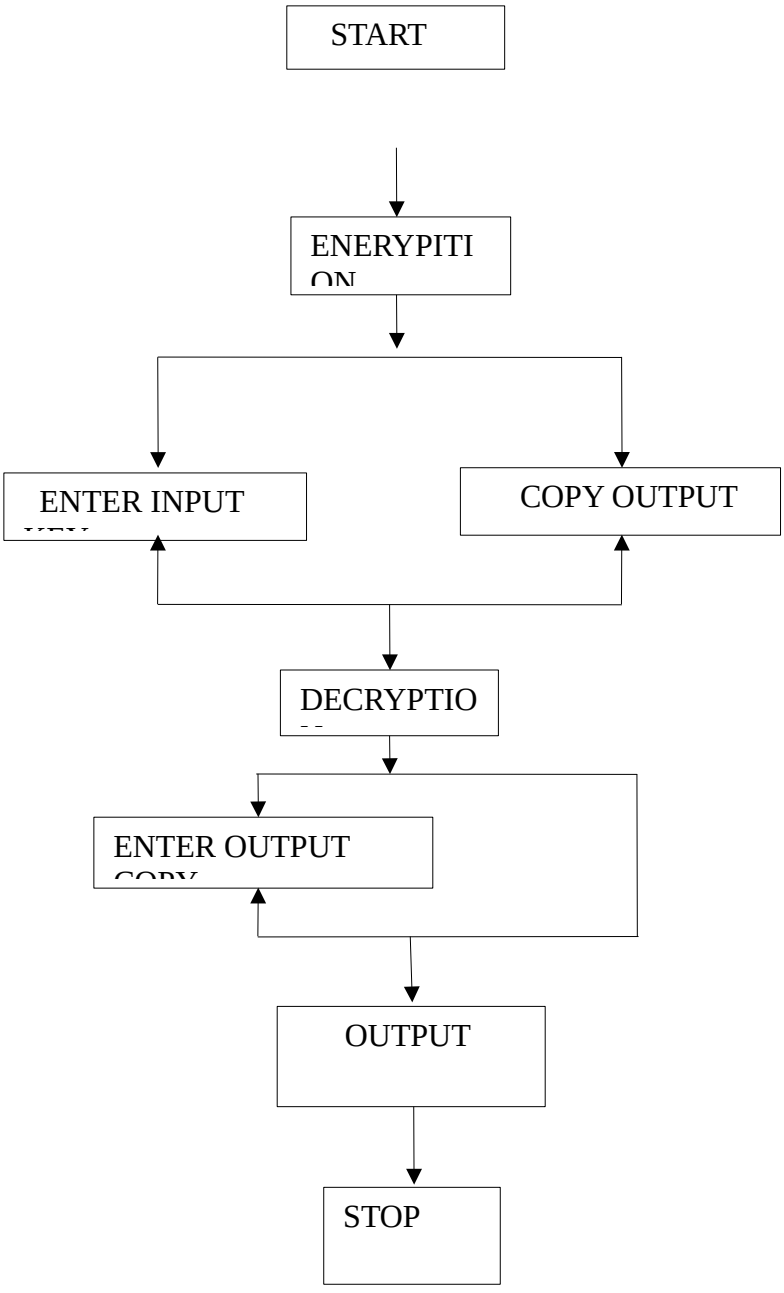
- **The Insecurity of Standard RBG**

Standard Random-Bit Generators (RBGs) are typically used to generate random bits in software/hardware using a Linear Congruential Generator (LCG). One of the most commonly used is the Knuth's LCG [15]. It was shown by Belarre et al. [4] that the secret-key of DSA can be recovered if the nonce is generated by Knuth's linear congruential generator with known parameters. This attack is provable and relies on Babai's approximation algorithm [5], based on the LLL algorithm [6]. Howgrave-Graham and Smart [7] showed that, even if the nonce is known only partially, i.e. only some of its bits are revealed, for a reasonable number of signatures, a number of heuristic attacks are possible to recover the secret-key. Finally, Nguyen and Shparlinski [8] presented a provable polynomial-time attack against DSA when the nonces are partially known, under two assumptions: the size of q should not be too small compared to p, and the probability of collisions for the hash function H should not be too large compared to 1/q. Under these conditions, if for a certain number of random messages μM and random nonces k[1,q-1], about log(1/2) q least significant bits of k are known, then in polynomial time, one can recover the signer's secret-key x.

3.2 DESIGN OF NEW SYSTEM

Caesar cipher

The Caesar cipher is a classic example of ancient cryptography and is said to have been used by Julius Caesar. The Caesar cipher is based on transposition and involves shifting each letter of the plaintext message by a certain number of letters, historically three. The ciphertext can be decrypted by applying the same number of shifts in the opposite direction. This type of encryption is known as a substitution cipher, due to the substitution of one letter for another in a consistent fashion.

- 

3.4 ADVANTAGES OF THE NEW SYSTEM OVER THE EXISTING SYSTEM

1.0 ADVANTAGE OF CAESAR CIPHER

- One of the easiest methods to use in cryptography and can provide minimum security to the information
- Use of only a short key in the entire process
- One of the best methods to use if the system cannot use any complicated coding techniques
- Requires few computing resources

1.1 DISADVANTAGES OF CAESER CIPHER

- Simple structure usage
- Can only provide minimum security to the information
- Frequency of the letter pattern provides a big clue in deciphering the entire message

2.1 ADVANTAGE OF RSA

- It is very easy to implement RSA algorithm.
- RSA algorithm is safe and secure for transmitting confidential data.
- Cracking RSA algorithm is very difficult as it involves complex mathematics.
- Sharing public key to users is easy.

2.2 DISADVANTAGE OF RSA

- It may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses asymmetric encryption only.

- It has slow data transfer rate due to large numbers involved.

- It requires third party to verify the reliability of public keys sometimes.

- High processing is required at receiver’s end for decryption.

- RSA can’t be used for public data encryption like election voting.