Privileged Cryptography

Abhishek Dhull[*], Priti[**]
*(Department of Computer Science & Applications, M.D. University, India)
** (Asstt. Prof., Department of Computer Science & Applications, M.D. University, India)

***ABSTRACT**: Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. This paper presents the way of protecting the information from:*

- *Intruders: those who capture the packet and alter the information.*
- *Cryptanalysts: those who decrypt cipher text into plain text without key.*

Keywords: *Cryptanalyst, Decryption, Encryption, Intruder, Private key, Public key.*

I. INTRODUCTION

Modern cryptography is heavily based on mathematical theory and computer science practice. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms. Until modern times 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" [6]. This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key[2]. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, *code* has a more specific meaning. It means the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, wallaby replaces attack at dawn). Codes are no longer used in serious cryptography—except incidentally for such things as unit designations (e.g., Bronco Flight or Operation Overlord)—since properly chosen ciphers are both more practical and more secure than even the best codes and also are better adapted to computers.

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.

II. EXISTING WAYS OF CRYPTOGRAPHY

Some use the terms *cryptography* and *cryptology* interchangeably in English, while others (including US military practice generally) use *cryptography* to refer specifically to the use and practice of cryptographic techniques and *cryptology* refer to the combined study of cryptography and cryptanalysis [3]. English is more flexible than several other languages in which *cryptology* (done by cryptologists) is always used in the second sense above.

2.1 Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976
One round (out of 8.5) of the patented IDEA cipher, used in some versions of PGP for high-speed encryption of, for instance, e-mail 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 (though DES's designation was finally withdrawn after the AES was adopted). 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. Many other block ciphers have been designed and released, with considerable variation in quality.

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. Block ciphers can be used as stream ciphers.

2.2 Symmetric-key algorithms

Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both encryption of plaintext and decryption of cipher text. Symmetric algorithms, sometimes called Conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa [1, 4]. The encryption key is trivially related to the decryption key, in that they may be identical or there is a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. Other terms for symmetric-key encryption are secret-key, single-key, shared-key, one-key, and private-key encryption. Use of the last and first terms can create ambiguity with similar terminology used in public-key cryptography. Symmetric-key cryptography is to be contrasted with asymmetric-key cryptography [8].

2.3 Types of symmetric-key algorithms:

Symmetric-key encryption can use either stream ciphers or block ciphers.

- Stream ciphers encrypt the bits of a message one at a time.
- Block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks [7].

2.3.1 Basic algorithm and terminology

RSA encryption and decryption are essentially mathematical operations. They are what are termed *exponentiation*, *modulo* a particular number. Because of this, RSA keys actually consist of numbers involved in this calculation, as follows:

- the public key consists of the modulus and a public exponent; the private key consists of that same modulus plus a private exponent.

2.3.2 Security of Public Key Schemes

- like private key schemes brute force exhaustive search attack is always theoretically possible
- but keys used are too large (>512bits)
- The public-key algorithms are based on a known hard problem. The its just made too hard to do in practise
- RSA Problem: Given n=pq, with p and q primes. Find p and q.
- requires the use of very large numbers, hence is slow compared to private key schemes

2.3.3 Existing Cryptography

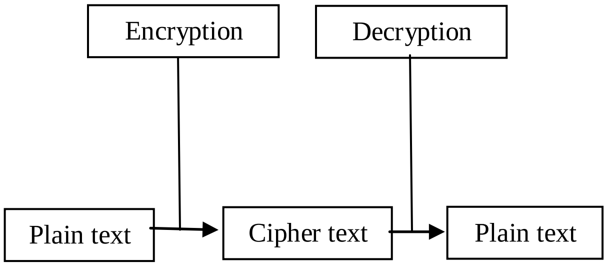

Fig. 1 Existing Cryptography

III. PROPOSED MODEL

3.1 Construction of Symmetric Ciphers

Many modern block ciphers are based on a construction proposed by Horst Feistel. Feistel's construction makes it possible to build invertible functions from other functions that are themselves not invertible.

3.2 Security of Symmetric Ciphers

Construction of the functions for each round can greatly reduce the chances of a successful attack.

3.3 Key Generation

When used with asymmetric ciphers for key transfer, pseudorandom key generators are nearly always used to generate the symmetric cipher session keys. However, lack of randomness in those generators or in their initialization vectors is disastrous and has led to cryptanalytic breaks in the past. Therefore, it is essential that an implementation uses a source of high entropy for its initialization. Symmetric ciphers have historically been susceptible to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis and linear cryptanalysis.

3.3.1 Detection of Intruder's Activity

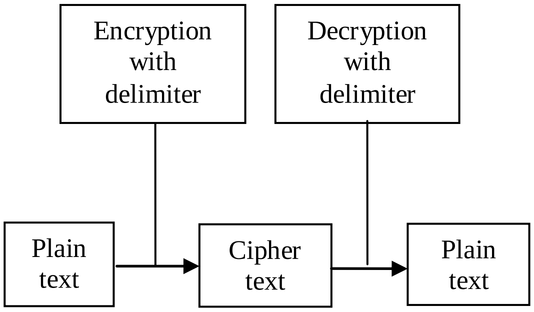

Fig.2 Encryption and Decryption with delimiter

Some time intruder make change in cipher text as a result it becomes difficult to know. Information becomes meaningless. A delimiter can be set with plain text during encryption so that at the time of decryption user could know whether cipher text was altered or not. If it is altered delimiter will not be visible at receiving end and packet will be retransmitted

3.3.2 Privileged Cryptography with IP Filtering

To protect information from cryptanalyst IP Filter would be attached in decryption module

Sometime cryptanalyst decrypt information without key, this problem can be solved using IP filtering

If there is decryption request from different IP then packets will be deleted.

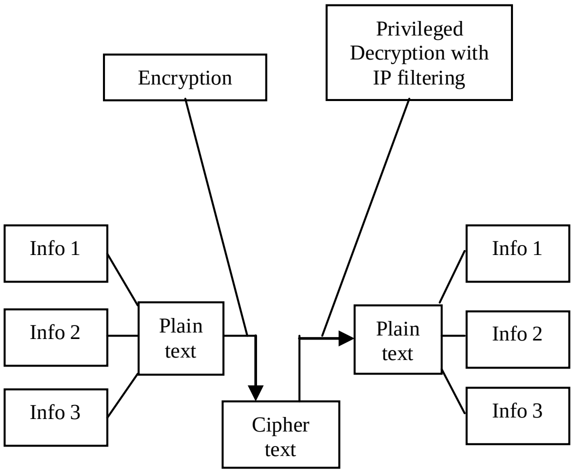

Fig. 3 Decryption with IP filtering

IV. CONCLUSION

It will improve the security of the text while sending it from sender to receiver. A delimiter can be set during encryption and decryption to know whether the data has been altered by an intruder or not. We can also protect our information from cryptanalyst, who can decrypt information without using key, by attaching IP filter during decryption. Hence our data becomes more secure when transmitted from sender to receiver.

REFERENCES

[1] Bruce Schneier, *Applied Cryptography*, 2nd ed.

[2] C.M. Adams, *Simple and Effective Key Scheduling for Symmetric Ciphers*, Workshop on Selected Areas in Cryptography-Workshop Record, Kingston, Ontario, May 1994, pp.129-133.

[3] C.M.Adams and H.Meijer, *Security-Related Comments Regarding McEliece's Public-Key Cryptosystem*, Advances in Cryptology-CRYPTO'87 Proceedings, Sringer-Verlag, 1988, pp. 224-230.

[4] B.S Adiga and P.Shankar, *Modified Lu-Lee Cryptosystem*, Electronics Letters, v.21, n.18, 29 Aug 1985, pp.794-795.

[5] L.M. Adleman, *On Breaking Generalized Knapsack Public Key Cryptosystems*, Proceedings of the 15th ACM Symposium on Theory of Computing, 1983, pp.402-412.

[6] Matt Blaze, *Cryptology and Physical Security: Rights Amplification in Master Keyed Mechanical Locks*, IEEE Security and Privacy, March 2003.

[7] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, and S.A. Vanstone, *An Implementatin for a Fast Public-Key Cryptosystem*, Journal of Cryptology, v.3, n. 2, 1991, pp. 63-79.

[8] G.B. Agnew, *Random Sources for Cryptographic Systems*, Advances in Cryptology- Eurocrypt'87 Proceedings, Springer-Verlag, 1988, pp. 77-81.