ISSN: 2394-7659
IMPACT FACTOR- 3.775

International Journal of Engineering Researches and Management Studies

THE CRYPTOGRAPHY

M.PRSANNA KUMAR[*1] & A.STALIN[2]
[*1&2]B.sc Computer Science VLBJCAS, Kovaipudur

ABSTRACT

This paper examines proposals for three cryptographic primitives: block ciphers, stream ciphers, and hash functions. It provides an overview of the design principles of a large number of recent proposals, which includes the global structure, the number of rounds, the way of introducing non-linearity and diffusion, and the key schedule. The software performance of about twenty primitives is compared based on highly optimized implementations for the Pentium. The goal of the paper is to provide a technical perspective on the wide variety of primitives that exist today

1. INTRODUCTION

Human being from ages had two inherent needs: (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypton' meaning hidden and 'grapheme' meaning writing.

2. HISTORY OF CRYPTOGRAPHY

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.The roots of cryptography are found in Roman and Egyptian civilizations.

3. HIEROGLYPH − THE OLDEST CRYPTOGRAPHIC TECHNIQUE

The first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph. This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such hieroglyph is shown below.Later, the scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC. This involved replacing alphabets of message with other alphabets with some secret rule. This **rule** became a **key** to retrieve the message back from the garbled message.The earlier Roman method of cryptography, popularly known as the **Caesar Shift Cipher,** relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.

4. STEGANOGRAPHY

Steganography is similar but adds another dimension to Cryptography. In this method, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists. For example, invisible watermarking.In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS

International Journal of Engineering Researches and Management Studies

5. EVOLUTION OF CRYPTOGRAPHY

- It is during and after the European Renaissance, various Italian and Papal states led the rapid proliferation of cryptographic techniques. Various analysis and attack techniques were researched in this era to break the secret codes.
- Improved coding techniques such as Vigenere Coding came into existence in the 15th century, which offered moving letters in the message with a number of variable places instead of moving them the same number of places.
- Only after the 19th century, cryptography evolved from the ad hoc approaches to encryption to the more sophisticated art and science of information security.
- In the early 20th century, the invention of mechanical and electromechanical machines, such as the Enigma rotor machine, provided more advanced and efficient means of coding the information.
- During the period of World War II, both cryptography and cryptanalysis became excessively mathematical.
- With the advances taking place in this field, government organizations, military units, and some corporate houses started adopting the applications of cryptography. They used cryptography to guard their secrets from others. Now, the arrival of computers and the Internet has brought effective cryptography within the reach of common people.

6. CRYPTOGRAPHY DEFINITION

- The science of coding and decoding messages so as to keep these messages secure. Coding (*see* encryption) takes place using a key that ideally is known only by the sender and intended recipient of the message.
- ***Note*** : Historically used in warfare, cryptography is now used routinely in computer networks. This often pits the desire of individuals and businesses to keep Internet information private against the need of government to investigate crime and terrorism.

7. THE BASIC PRINCIPLES OF MODERN CRYPTOGRAPHY

The previous section has given a taste of historical cryptography. It is fair to say that, historically, cryptography was more of an art than any sort of science: schemes were designed in an ad-hoc manner and then evaluated based on their perceived complexity or cleverness. Unfortunately, as we have seen, all such schemes (no matter how clever) were eventually broken. Modern cryptography, now resting on firmer and more scientific foundations, gives hope of breaking out of the endless cycle of constructing schemes and watching them get broken. In this section we outline the main principles and paradigms that distinguish modern cryptography from classical cryptography. We identify three main principles:

- Principle 1 — the first step in solving any cryptographic problem is the formulation of a rigorous and precise definition of security.
- Principle 2 — when the security of a cryptographic construction relies on an unproven assumption, this assumption must be precisely stated. Furthermore, the assumption should be as minimal as possible.
- Principle 3 — cryptographic constructions should be accompanied by a rigorous proof of security with respect to a definition formulated according to principle 1, and relative to an assumption stated as in principle 2 (if an assumption is needed at all).

8. TYPES OF CRYPTOGRAPHY

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system:

- ✓ **Symmetric Key Encryption**
- ✓ **Asymmetric Key Encryption**

ISSN: 2394-7659
IMPACT FACTOR- 3.775

International Journal of Engineering Researches and Management Studies

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are
closely associated. It is practically impossible to decrypt the ciphertext with the key that
is unrelated to the encryption key.

9. SYMMETRIC KEY ENCRYPTION

The encryption process where same keys are used for encrypting and decrypting theinformation is known as Symmetric Key Encryption..The study of symmetric cryptosystems is referred to as symmetric cryptography.Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.A few well-known examples of symmetric key encryption methods are:

Digital EncryptionStandard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.
Cryptography Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

10. THE SALIENT FEATURES OF CRYPTOSYSTEM BASED ON SYMMETRIC KEY ENCRYPTION ARE

- ✓ Persons using symmetric key encryption must share a common key prior to
- ✓ exchange of information.
- ✓ Keys are recommended to be changed regularly to prevent any attack on the
- ✓ system.
- ✓ A robust mechanism needs to exist to exchange the key between the
- ✓ communicating parties. As keys are required to be changed regularly, this
- ✓ mechanism becomes expensive and cumbersome.
- ✓ In a group of n people, to enable two-party communication between any two
- ✓ persons, the number of keys required for group is $n \times (n – 1)/2$.
- ✓ Length of Key (number of bits) in this encryption is smaller and hence, process of
- ✓ encryption-decryption is faster than asymmetric key encryption.
- ✓ Processing power of computer system required to run symmetric algorithm is less.
- ✓ Challenge of Symmetric Key Cryptosystem
- ✓ There are two restrictive challenges of employing symmetric key cryptography.
- ✓ Key establishment – Before any communication, both the sender and the receiver
- ✓ need to agree on a secret symmetric key. It requires a secure key establishment
- ✓ mechanism in place.
- ✓ Trust Issue – Since the sender and the receiver use the same symmetric key,
- ✓ there is an implicit requirement that the sender and the receiver ‘trust’ each other.
- ✓ For example, it may happen that the receiver has lost the key to an attacker and
- ✓ the sender is not informed.

11. CRYPTOGRAPHY

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

12. ASYMMETRIC KEY ENCRYPTION

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration: Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows:

ISSN: 2394-7659
IMPACT FACTOR- 3.775

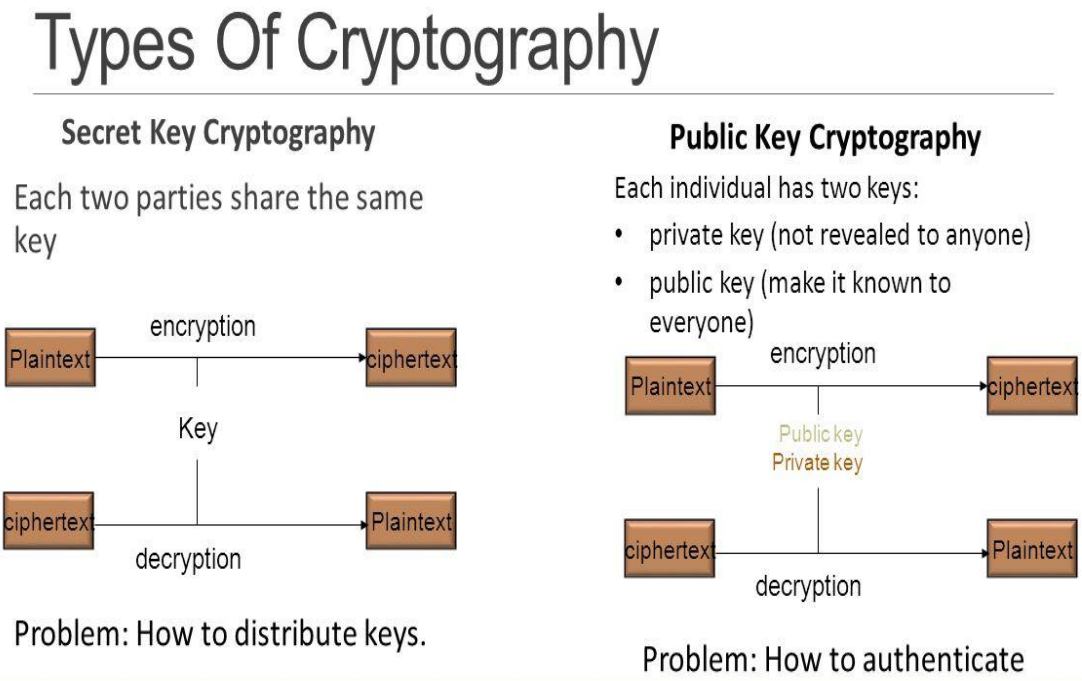
International Journal of Engineering Researches and Management Studies

- Every user in this system needs to have a pair of dissimilar keys, private key and
- public key. These keys are mathematically related – when one key is used for
- encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a wellguarded
- secret. Hence, this scheme of encryption is also called Public Key
- Encryption.
- Though public and private keys of the user are related, it is computationally not
- feasible to find one from another. This is a strength of this scheme.
- When Host1 needs to send data to Host2, he obtains the public key of Host2 from
- repository, encrypts the data, and transmits.
- Host2 uses his private key to extract the plaintext.
- Cryptography
- 12
- Length of Keys (number of bits) in this encryption is large and hence, the process
- of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is
- higher.
- Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems
- are quite difficult to comprehend.
- You may think, how can the encryption key and the decryption key are 'related', and yet
- it is impossible to determine the decryption key from the encryption key? The answer lies
- in the mathematical concepts. It is possible to design a cryptosystem whose keys have
- this property. The concept of public-key cryptography is relatively new. There are fewer
- public-key algorithms known than symmetric algorithms.
- Challenge of Public Key Cryptosystem
- Public-key cryptosystems have one significant challenge: the user needs to trust that the
- public key that he is using in communications with a person really is the public key of that
- person and has not been spoofed by a malicious third party.
- This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted
- third party. The third party securely manages and attests to the authenticity of public
- keys. When the third party is requested to provide the public key for any communicating
- person X, they are trusted to provide the correct public key.
- The third party satisfies itself about user identity by the process of attestation,
- notarization, or some other process - that X is the one and only, or globally unique, X. The
- most common method of making the verified public keys available is to embed them in a
- certificate which is digitally signed by the trusted third party.
- Relation between Encryption Schemes
- A summary of basic key properties of two types of cryptosystems is given below:
- Symmetric
- Cryptosystems
- Public Key Cryptosystems
- Relation between
- Keys
- Same Different, but mathematically
- related
- Encryption Key Symmetric Public
- Decryption Key Symmetric Private
- Due to the advantages and disadvantage of both the systems, symmetric key and publickey
- cryptosystems are often used together in the practical information security systems.

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS

International Journal of Engineering Researches and Management Studies



13. CRYPTOGRAPHIC PRIMITIVES

This paper focuses on the three most common cryptographic primitives: additive stream ciphers, cryptographic hash functions, and block ciphers. It will be assumed that the reader is familiar with the basic requirements for these primitives, as well as with the ways how these primitives can be used to provide security services such as confidentiality and authentication.

14. ADDITIVE STREAM CIPHERS

Additive stream ciphers stretch a short key and an initial value to a key-stream sequence. If data confidentiality is required, the sender will add this key-stream sequence to the data, simulating the operation of a one-time pad (but without the perfect secrecy). The recipient can recover the data by subtracting the same key-stream sequence. Additive stream ciphers are also known as pseudo-random string generators. The stream ciphers that are discussed here are 'alleged RC4,' SEAL, and WAKE. The cryptographic literature contains a large number of papers on other constructions derived from linear feedback shift registers (see for example [78]). Important examples include nonlinear filter functions and clock controlled shift registers. They are usually defined at bit level, which makes them more suited for hardware than for software. Although it is certainly possible to adopt these constructions to software environments, they will not be consideredinthispaper.

15. CRYPTOGRAPHIC HASH FUNCTIONS

Cryptographic hash functions compress strings of arbitrary lengths to strings of fixedlengths(typically64, 128or160bits).Inaddition,theysatisfythefollowing properties [54,65]: – preimage resistance: it should be hard to find a preimage for a given hash result; – 2nd preimage resistance: it should be hard to find a 2nd preimage for a given input.

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS

International Journal of Engineering Researches and Management Studies

16. MODERN CRYPTOGRAPHY CONCERNS ITSELF WITH THE FOLLOWING FOUR OBJECTIVES

- ✓ **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)
- ✓ **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
- ✓ **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information).

17. CONCLUSIONS

At present, it is not possible to design a additive stream cipher, hash function, or block cipher which is both very fast and 'secure'. This can be summarized in the following quotes:

L. O'Connor: "Most ciphers are secure after sufficiently many rounds." J.L. Massey: "Most ciphers are too slow after sufficiently many rounds."

Some progress has been made into the direction of provable security, often at the cost of performance. What does exist however is provable insecurity, i.e., for some designs, serious weaknesses have been identified. Given the fact that most fast designs are still developed in a 'trial-and error paradigm' and that very little evaluation effort is available; the reader is cautioned against adopting new cryptographic primitives too quickly. While the cryptographic community has made significant progress during the last twenty years, our knowledge is still very limited; existing cryptanalytic results should be evaluated with great care, even if they are only of theoretical nature.

References

Web sites:

- ➢ www.epic.org
  Electronic Privacy Information Center.
- ➢ www.crypto.org
  Internet Privacy Coalition.
- ➢ www.eff.org
  Electronic Frontier Foundation.
- ➢ www.privacy.org
  Privacy.org. Great information resource about privacy issues.
- ➢ www.cdt.org
  Center for Democracy and Technology.
- ➢ www.philzimmermann.com
  Phil Zimmermann's home page, his Senate testimony, and so on.

Books:

- ✓ Privacy on the Line: The Politics of Wiretapping and Encryption, Whitfield Differ and Susan Landau, the MIT Press, 1998, ISBN 0-262-04167-7. This book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people. Includes information that even a lot of experts don't know.
- ✓ Technology and Privacy: The New Landscape, Philip Agre and Marc Rotenberg, the MIT Press, 1997; ISBN 0-262-01162-x.
- ✓ Building in Big Brother, The Cryptographic Policy Debate, edited by Lance Hoff-man, Springer-Verlag, 1995; ISBN 0-387-94441-9.
- ✓ The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand How the human need for privacy has manifested itself through cryptography.