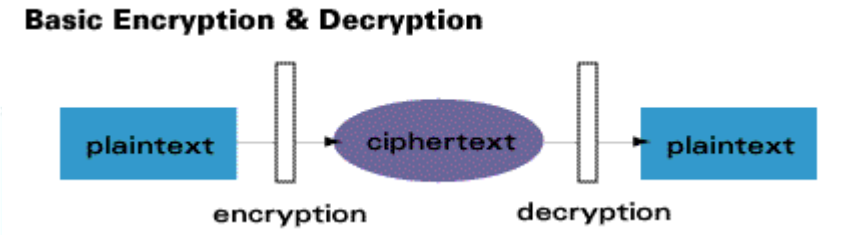
CRYPTOGRAPHIC ANALYSIS

Mrs. Yashita Jain
Asst. Prof., Department of Mathematics, Khalsa College for Women, Ludhiana (India)

ABSTRACT
To keep the information secret, there are two possible strategies: hide the existence of the information, or make the information unintelligible. Cryptography is the art and science of keeping information secure from unintended audiences, of encrypting it. Conversely, cryptanalysis is the art and science of breaking encoded data. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology.
Cryptography provides for secure communication in the presence of malicious third-parties—known as adversaries. Encryption (a major component of cryptography) uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Modern cryptography uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt the data.



Today, cryptography is used to provide secrecy and integrity to our data, and both authentication and anonymity to our communications.

KEYWORDS
encryption, decryption, symmetric, asymmetric, keys, cipher text, plain text, integrity.

INTRODUCTION

Does increased security provide comfort to people? During this time when the Internet provides essential communication between literally billions of people and is used as a tool for commerce, social interaction, and the exchange of an increasing amount of personal information, security has become a tremendously important issue for every user to deal with.
There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting health care information. One essential aspect for secure communications is that of cryptography. It is to notice that cryptography is necessary for secure communications, not sufficient. Here, in the present paper, there is the discussion of the few initial steps necessary for better security in any of the situations. Here, some of the terminology and concepts behind cryptography are discussed.

HISTORY OF CRYPTOGRAPHY

Cryptology was a public field in the United States until World War I, when the Army & Navy realized its value to national security and began working in secret. Through the early 1970s, cryptology was dominated by the government both because computers were very expensive and because the government released very little information. It returned to mainstream academic and scientific communities in a sort of cryptology renaissance when the computer revolution made computers more readily available and when demand for encryption increased due to fundamental changes in the ways America communicated.

The increase in demand for cryptography was driven by industry interest for financial services, securing electronic transactions and securing trade secrets stored on computers), and individually for securing wireless communications. Digital communications were obvious candidates for encryption.

PRINCIPLES OF CRYPTOGRAPHY

Modern cryptographers emphasize that security should not depend on the secrecy of the encryption method (or algorithm), only the secrecy of the keys. The secret keys must not be revealed when plaintext and ciphertext are compared, and no person should have knowledge of the key. Modern algorithms are based on mathematically difficult problems - for example, prime number factorization, discrete logarithms, etc. There is no mathematical proof that these problems are in fact are hard, just empirical evidence.

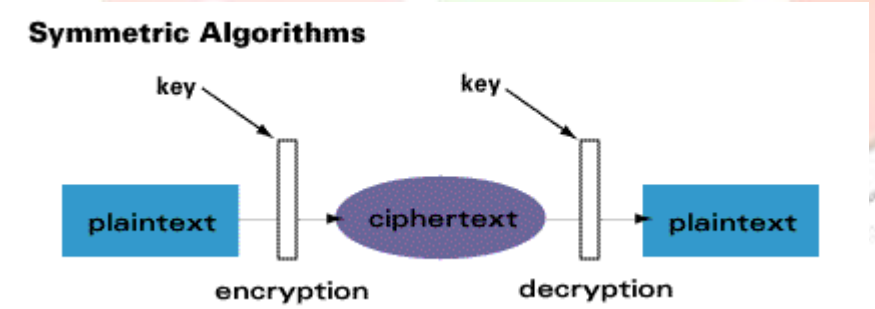
Modern cryptographic algorithms are too complex to be executed by humans. Today's algorithms are executed by computers or specialized hardware devices, and in most cases are implemented in computer software.

The design of secure systems using encryption techniques focuses mainly on the protection of (secret) keys. Keys can be protected either by encrypting them under other keys or by protecting them physically, while the algorithm used to encrypt the data is made public and subjected to intense scrutiny. When cryptographers hit on an effective method of encryption (a cipher), they can patent it as intellectual property and earn royalties when their method is used in commercial products. In the current open environment, many good cryptographic algorithms are available in major bookstores, libraries and on the Internet, or patent office.

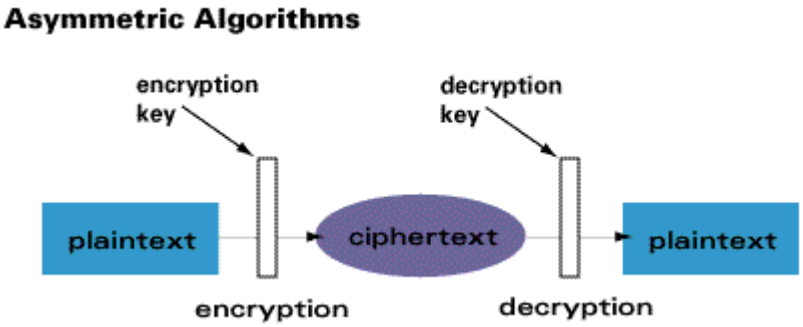
TYPES OF CRYPTOGRAPHIC KEYS

There are two types of key-based encryption, symmetric (or secret-key) and asymmetric (or public-key) algorithms. Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), while asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.



Asymmetric ciphers (also called public-key cryptography) make a public key universally available, while only one individual possesses the private key. When data is encrypted with the public key, it can only be decrypted with the private key, and vice versa. Public key cryptography adds a very significant benefit - it can serve to authenticate a source (e.g. a digital signature). Public key cryptography was invented by Whitfield Diffie and Martin Hellman in 1975.



In general, symmetric algorithms execute much faster than asymmetric ones. In real applications, they are often used together, with a public-key algorithm encrypting a randomly generated encryption key, while the random key encrypts the actual message using a symmetric algorithm. This combination is commonly referred to as a digital envelope.

PRIMARY FUNCTIONS OF CRYPTOGRAPHY

Cryptography is the science of secret writing is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard algorithms in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic notes to war-time battle plans. New forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. There are five primary functions of cryptography today:

1. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
2. Authentication: The process of proving one's identity.
3. Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
4. Non-repudiation: A mechanism to prove that the sender really sent this message.
5. Key exchange: The method by which crypto keys are shared between sender and receiver.

In cryptography, we start with the unencrypted data, referred to as plaintext. Plaintext is encrypted into ciphertext, which will in turn (usually) be decrypted back into usable plaintext. The encryption and decryption is based upon the type of cryptography scheme being employed and some form of key. For those who like formulas, this process is sometimes written as:

$$C=E_k(P)$$
$$P= D_k(C)$$

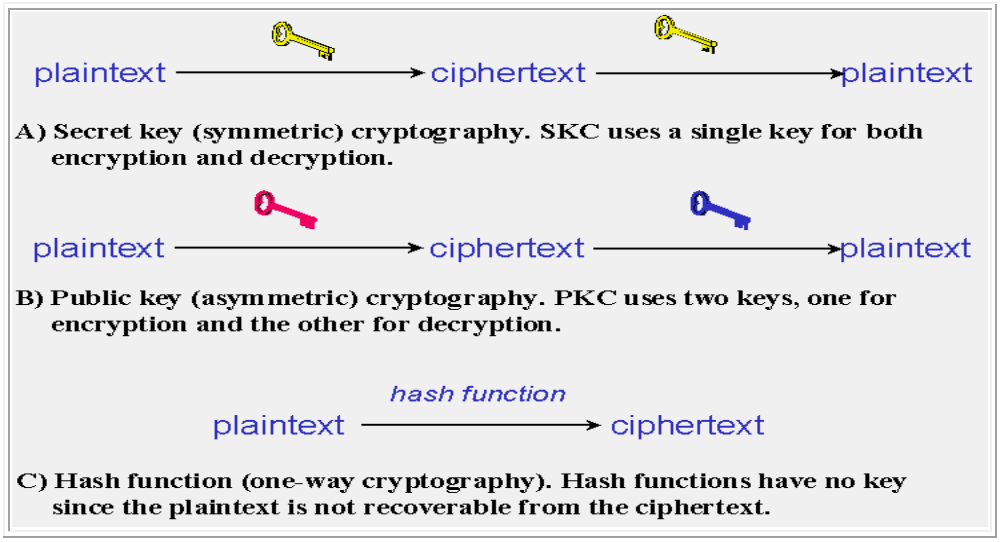
where **P** = plaintext, **C** = ciphertext, **E** = the encryption method, **D** = the decryption method, and **k** = the key.

Finally, cryptography is most closely associated with the development and creation of the mathematical algorithms used to encrypt and decrypt messages, whereas cryptanalysis is the science of analyzing and breaking encryption schemes. Cryptology is the term referring to the broad study of secret writing, and encompasses both cryptography and cryptanalysis.

TYPES OF CRYPTOGRAPHIC ALGORITHM

There are several ways of classifying cryptographic algorithms. These will be categorized based on the number of keys that are employed for encryption and decryption.The three types of algorithms that will be discussed are

- **Secret Key Cryptography (SKC)**: Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.
- **Public Key Cryptography (PKC)**: Uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.
- **Hash Functions**: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.



Public Key Cryptography (PKC)

PKC depends upon the existence of so called one way or mathematical functions that are easy to compute whereas their inverse functions are relatively difficult to compute. The mathematical "trick" in PKC is to find a trap door in the one-way function so that the inverse calculation becomes easy given knowledge of some item of information.

PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. The important point here is that it does not matter which key is applied first, but that both keys are required for the process to work. Because, a pair of keys are required, this approach is also called asymmetric cryptography. One of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party.

Secret Key Cryptography (SKC)

SKC schemes are generally categorised as being either stream chippers or block chippers. Stream chippers operate on a single bit at a time, so this key is constantly changing. A block chipper encrypts one block of data at a time using the same key on each block. Secret key cryptography methods employ a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Hash Function

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if

input data is unknown, it is very difficult to reconstruct by knowing the stored hash value. Hash functions, also called message digests and one-way encryption, are algorithms that, in essence, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents , often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a mechansim to ensure the integrity of a file.

Hash functions are sometimes misunderstood and some sources claim that no two files can have the same hash value. Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence.

CONCLUSIONS

This paper is a discussion on how digital cryptography works. There are a number of ways to attack every one of these systems. In the words of Sherlock Holmes, "What one man can invent, another can discover".

Cryptography is particularly interesting field because of the amount of work is being kept secret. The logic behind it is that secrecy is not the key to the goodness of a cryptographic algorithm. Inspiteof the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied. In fact, *time* is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice of keys.

REFERENCES

1. Oded Goldreich Cambridge 2001. Foundations of cryptography (basic tools)
2. Oded Goldreich, Springer-Verlag 1998 Modern Cryptography, Probabilistic Proofs and Pseudorandomness
3. WilliamsStallings Cryptography and Network Security: Principles and Practice.
4. Douglas R. Stinson. Cryptography: Theory and Practice.
5. Dominic Welsh, Oxford: Clarendon press, England, Codes and Cryptography
6. Johannes A Buchman, Introduction to Cryptography.
7. Brands,Springer-Verlag 1994, Advances in cryptology-proceedings of crypto.
8. Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.
9. Ferguson, N., & Schneier, B. (2003). Practical Cryptography. New York: John Wiley & Sons.
10. Grabbe, J.O. (1997, October 10). Cryptography and Number Theory for Digital Cash.
11. Koblitz, N. (1994). A Course in Number Theory and Cryptography, 2nd ed. New York: Springer-Verlag.
12. Mao, W. (2004). Modern Cryptography: Theory & Practice. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference.