THE SCIENCE OF CRYPTOSYSTEM WITH MATHEMATICS

Satish*

ABSTRACT

Cryptography *is the study of information hiding and verification. It includes the protocols, algorithms and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication.*

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, integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols.

The basic terminology is that cryptography refers to the science and art of designing ciphers; cryptanalysis to the science and art of breaking them; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the ciphertext. Thereafter, things get somewhat more complicated. There are a number of cryptographic primitives—basic building blocks, such as block ciphers, stream ciphers, and hash functions. Block ciphers may either have one key for both encryption and decryption, in which case they're called shared key (also secret key or symmetric), or have separate keys for encryption and decryption, in which case they're called public key or asymmetric. A digital signature scheme is a special type of asymmetric crypto primitive.

Keywords: *Cryptography, Encryption, Decryption, Ciphertext, Plaintext.*

*Extension lecturer, govt P.G College, Jind

INTRODUCTION:

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Go check your e-mail. You'll notice that the webpage address starts with \https://". The \s" at the end stands for \secure" meaning that a process called SSL is being used to encode the contents of your inbox and prevent people from hacking your account. The heart of SSL { as well as pretty much every other computer security or encoding system { is something called a public key encryption scheme

GOALS OF CRYPTOGRAPHY

Security Services: If we are taking about security of information then following services come in mind.

1. Confidentiality (privacy)
2. Authentication (who created or sent the data)
3. Integrity (has not been altered)
4. Non-repudiation (the order is final)
5. Access control (prevent misuse of resources)
6. Availability (permanence, non-erasure)

1. message **confidentiality** (or privacy): Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information.

2. sender **authentication**: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled (or combinations) so to validate claims from emitter or to validated the recipient expectations.
3. message **integrity**: The recipient should be able to determine if the message has been altered.
4. sender **non-repudiation**: The emitter should not be able to deny sending the message.

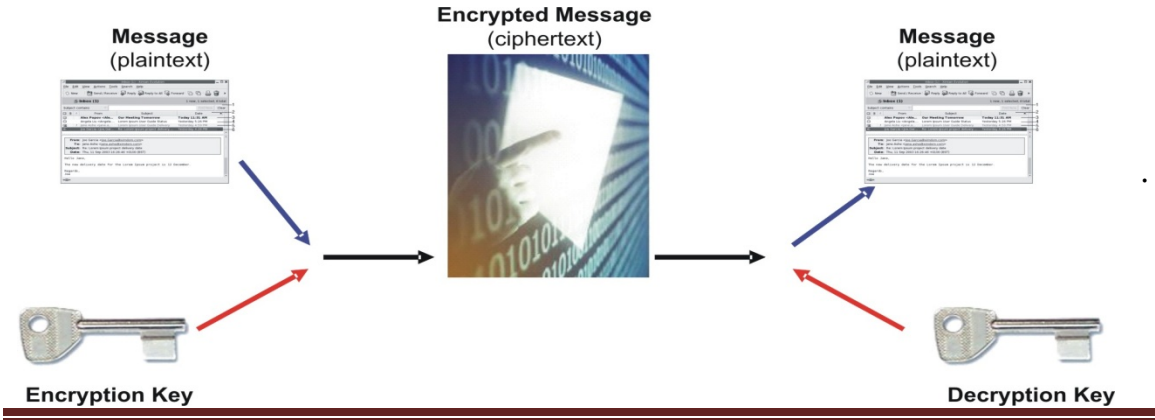
Not all cryptographic systems achieve all of the above goals. Some applications of cryptography have *different* goals; for example some situations require **repudiation** where a participant can plausibly deny that they are a sender or receiver of a message, or extend these goals to include variations like:

1. message **access control**: Who are the valid recipients of the message.
2. message **availability**: By providing means to limit the validity of the message, channel, emitter or recipient in time or space.

FORMS OF CRYPTOGRAPHY:

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three forms of algorithms that will be discussed are:

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption



In

cryptographic systems, the term *key* refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

Secret key cryptography is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. In addition, there is also the problem of how you communicate the secret key securely.

Public key cryptography, also called *asymmetric encryption*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.

The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key. The following example illustrates how public key cryptography works:

- Ann wants to communicate secretly with Bill. Ann encrypts her message using Bill's public key (which Bill made available to everyone) and Ann sends the scrambled message to Bill.
- When Bill receives the message, he uses his private key to unscramble the message so that he can read it.
- When Bill sends a reply to Ann, he scrambles the message using Ann's public key.
- When Ann receives Bill's reply, she uses her private key to unscramble his message.

In Mathematical terms A private-key cryptosystem consists of an encryption system E and a decryption system D. The encryption system E is a collection of functions E_K, indexed by ``keys" K, mapping some set of ``plaintexts" P to some set of ``ciphertexts" C. Similarly the decryption system D is a collection of functions D_K such that D_K(E_K(P)) = P for every plaintext P. That is, succesful decryption of ciphertext into plaintext is accomplished using the same key (index) as was used for the corresponding encryption of plaintext into ciphertext.

Such systems, where the same key value is used to encrypt and decrypt, are also known as ``symmetric'' cryptoystems.

Most cryptographic algorithms use keys, which are mathematical values that plug into the algorithm. If the algorithm says to encipher a message by replacing each letter with its numerical equivalent (A = 1, B = 2, and so on) and then multiplying the results by some number X, X represents the key to the algorithm. If the key is 5, \attack," for example, turns into \5 100 100 5 15 55." With a key of 6, it becomes \6 120 120 6 18 66." (Nobody would actually use this cipher, though; all the resulting numbers are divisible by the key, which gives it away.) Cipher algorithms and cipher keys are like door locks and door keys. All the locks from a given company may work in the same way, but all the keys will be different.

In the notation above, a ciphertext-only attack is one where F is constant. Given only some information G(E_K(P_1),...,E_K(P_n)) about n ciphertexts, the attack has to have some chance of producing some information H(P_1,...,P_n) about the plaintexts. The attack is trivial

if it has just as good a chance of producing H(P_1,...,P_n) when given G(C_1,...,C_n) for random C_1,...,C_n.

For example, say G(C) = C, and say H(P) is the first bit of P. We can easily write down an attack---the ``guessing attack,'' which simply guesses that H(P) is 1. This attack is trivial because it doesn't use the ciphertext: it has a fifty-fifty chance of guessing correctly no matter what. On the other hand there is an attack on RSA which produces one bit of information about P, with 100% success, using C. If it is fed a random C then the success rate drops to 50%. So this is a nontrivial attack.

The classic known-plaintext attack has F(P_1,P_2) = P_1, G(C_1,C_2) = (C_1,C_2), and (P_1,P_2) depending only on P_2.

In other words, given two ciphertexts C_1 and C_2 and one decryption P_1, the known-plaintext attack should produce information about the other decryption P_2.

Note that known-plaintext attacks are often defined in the literature as producing information about the key, but this is pointless: the cryptanalyst generally cares about the key only insofar as it lets him decrypt further messages.

As an example, to be explained in more detail below, consider the message

24368951877405221493008950603 3

99859633578287983910705162536 0

714044805511493277120102735032 5,

323915666133187777174633743307

665741495158513587387621667442

845150659031218458417248222366 76

It was encrypted using the key

e = 5,

N = 519208104502047440191322024032

46112884629925425640897326550 8

51544998255968235697331455544257

The number N is the product of two primes, just as 39 is the product of the primes 3 and 13. If you could discover the primes, you could decrypt the message. But this is not so easy to do, and this is one of the reasons why RSA works.

Primes, factorization, and a a secret message to decode

1234567 = 127 x 9721

102003000400005000006000000 7 = ? x ? x ? ...

public key = 5, 519208104502047440191322024032

46112884629925425640897326550 8 51544998255968235697331455544257

secret message = 243689518774052214930089506033

998596335782879839107051625360714044805511493277120102735032 5,

323915666133187777174633743307665741495158513587387621667442

845150659031218458417248222366 76 =???

PROBLEMS WITH CRYPTOGRAPHY:

The hard problems have been categorized into the following themes:

- Discrete Logarithms: Hard problems related to the discrete logarithm problem in cyclic groups.
- Factoring: Hard problems related to factoring.
- Product Groups: Hard problems related to the discrete logarithm problem in direct products of cyclic groups.
- Pairings: Hard problems related to pairings.
- Lattices: Hard problems related to lattices.

- Miscellaneous: Any problem that does not fit in the above. We will create new sub-domains if necessary.

REFERENCES:

1. D. Micciancio. Improving lattice based cryptosystems using the Hermite normal form. In Cryptography and Lattices (Providence, RI, 2001), volume 2146 of Lecture Notes in Comput. Sci., pages 126–145. Springer, Berlin, 2001.
2. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31(4):469–472, 1985.
3. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Information Theory, IT-22(6):644–654, 1976.
4. D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than N 0.292 dvances in Cryptology—EUROCRYPT ’99 (Prague), volume 1592 of Lecture Notes in Comput. Sci., pages 1–11. Springer, Berlin, 1999.
5. R. Crandall and C. Pomerance. Prime Numbers. Springer-Verlag, New York, 2001.
6. http://www.contrib.andrew.cmu.edu/~shadow/crypt/Cryptography_FAQ_(04_10:_Mathematical_Cryptology)