REPORT ON CRYPTOGRAPHY

Saakshi Agrawal
SY. BTECH. IT.
171081024
VJTI

Guided by Mr. Pranav Nerurkar
Dept. of CE & IT,
VJTI,
Mumbai

February 5, 2019

Contents

Chapter 1

Introduction

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext).Decryption is the reverse, in other words, moving from the unintelligible ciphertext 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". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext.

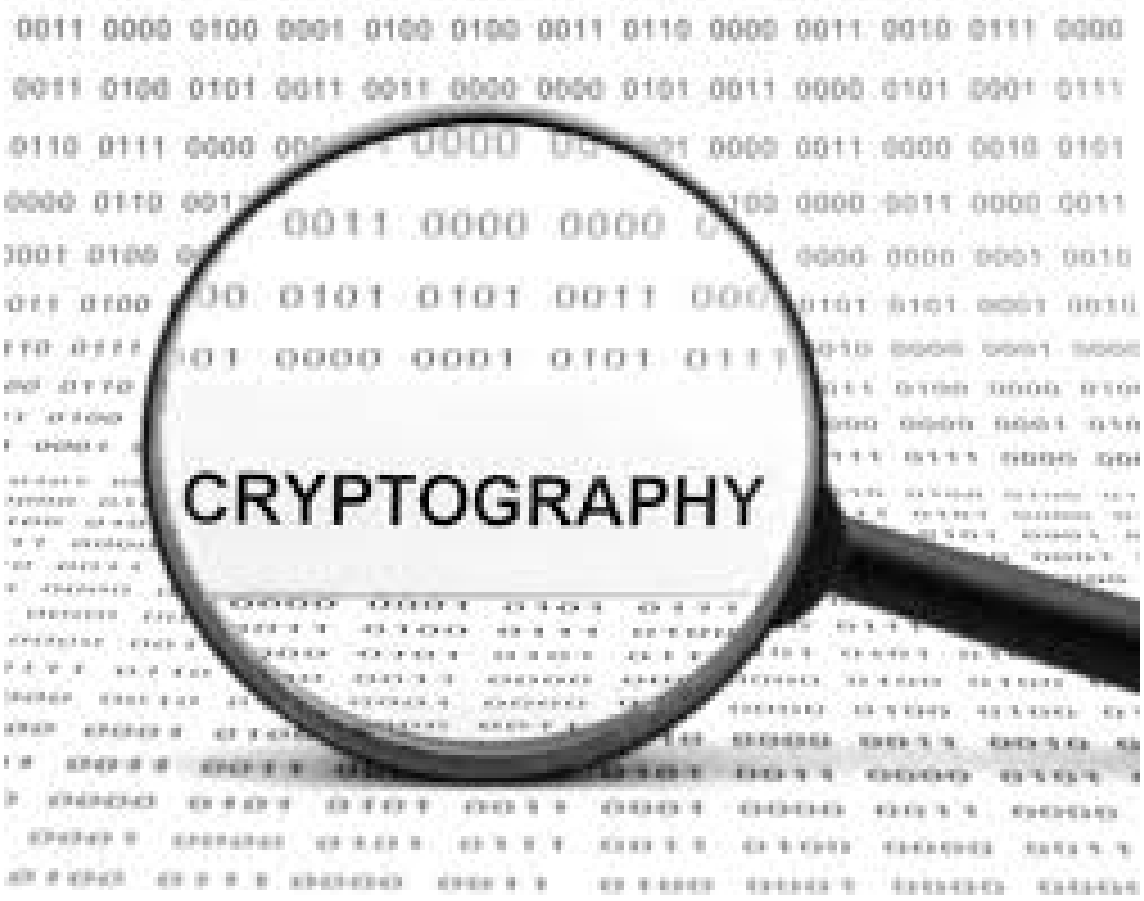

Figure 1.1: Cryptography [2]

Chapter 2

Types of Cryptography

1. Secret Key Cryptography

   Secret key cryptography methods employ a single key for both encryption and decryption. As shown in Figure 1A, 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 (more on that later in the discussion of public key cryptography).

   Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers.

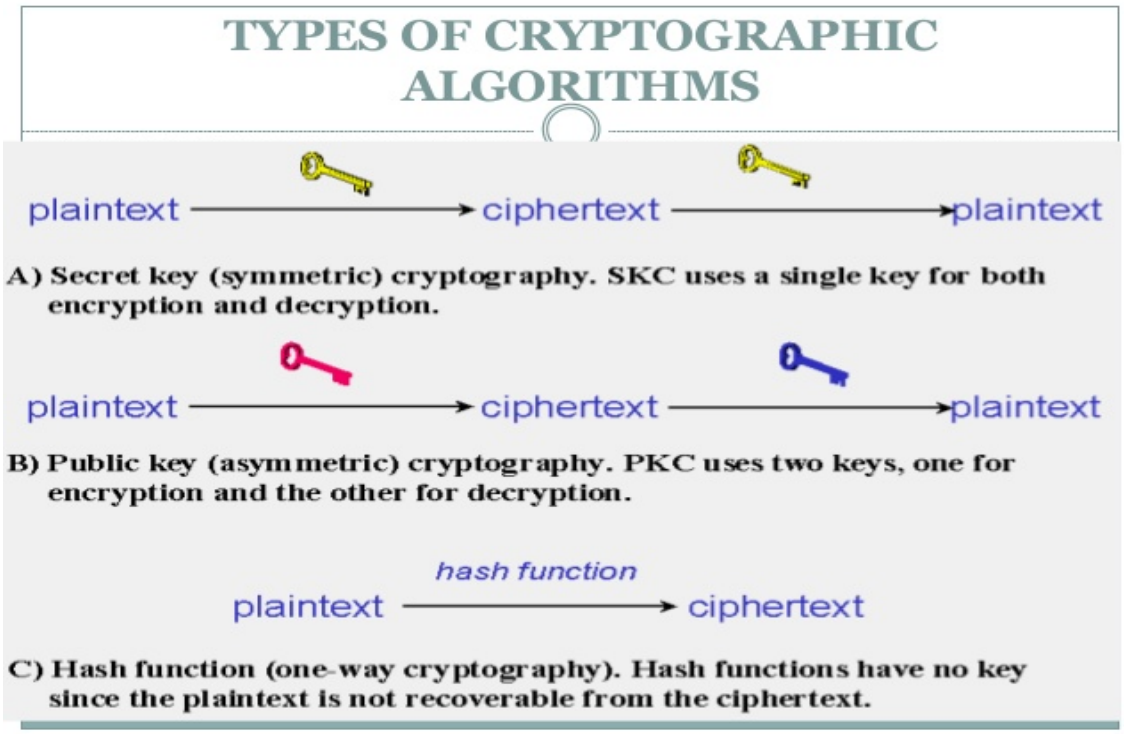

Figure 2.1: Secret Key Cryptography [3]

2. Public Key Cryptography

PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute. Let me give you two simple examples:

1. Multiplication vs. factorization: Suppose you have two prime numbers, 3 and 7, and you need to calculate the product; it should take almost no time to calculate that value, which is 21. Now suppose, instead, that you have a number that is a product of two primes, 21, and you need to determine those prime factors. You will eventually come up with the solution but whereas calculating the product took milliseconds, factoring will take longer. The problem becomes much harder if we start with primes that have, say, 400 digits or so, because the product will have 800 digits.

2. Exponentiation vs. logarithms: Suppose you take the number 3 to the 6th power; again, it is relatively easy to calculate $3^6 = 729$. But if you start with the number 729 and need to determine the two integers, x and y so that $\log_x 729 = y$, it will take longer to find the two values. While the examples above are trivial, they do represent two of the functional pairs that are used with PKC; namely, the ease of multiplication and exponentiation versus the relative difficulty of factoring and calculating logarithms, respectively. 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.

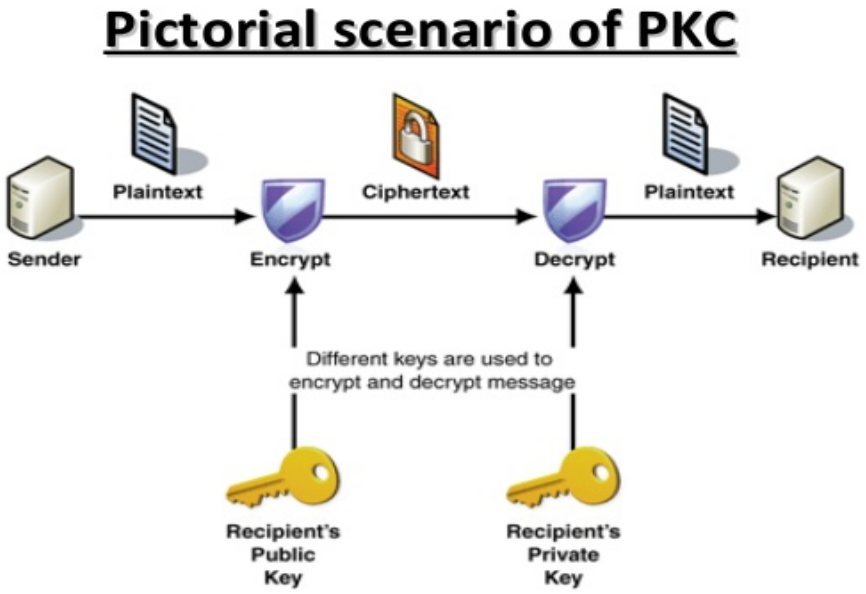

Figure 2.2: Public Key Cryptography [2]

3. Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in essence, use no key (Figure 1C). 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 mechanism to ensure the integrity of a file.

Note that these sites search databases and/or use rainbow tables to find a suitable string that produces the hash in question but one can't definitively guarantee what string originally produced the hash. Suppose that you want to crack someone's password, where the hash of the password is stored on the server. Indeed, all you then need is a string that produces the correct hash and you're in! However, you cannot prove that you have discovered the user's password, only a "duplicate key."

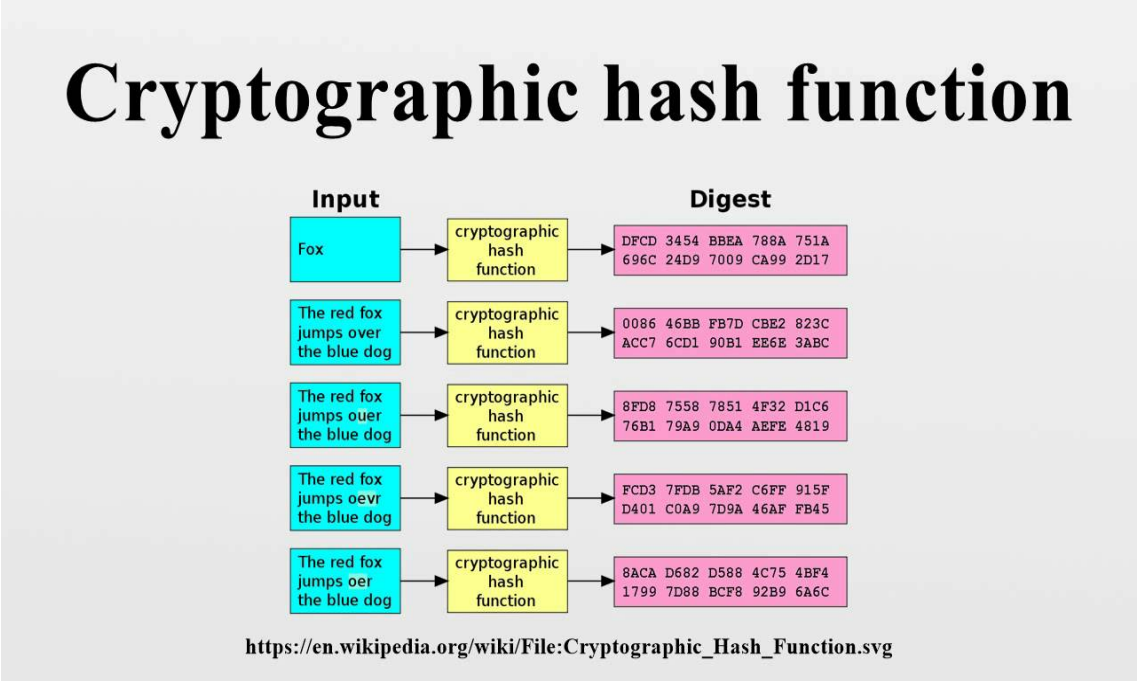

Figure 2.3: Hash Functions [3]

Chapter 3

Applications of Cryptography

1. Secrecy in Transmission: Most current secrecy systems for transmission use a private key system for transforming transmitted information because it is the fastest method that operates with reasonable assurance and low overhead.

If the number of communicating parties is small, key distribution is done periodically with a courier service and key maintenence is based on physical security of the keys over the period of use and destruction after new keys are distributed.

2. Secrecy in Storage: Secrecy in storage is usually maintained by a one-key system where the user provides the key to the computer at the beginning of a session, and the system then takes care of encryption and decryption throughout the course of normal use. As an example, many hardware devices are available for personal computers to automatically encrypt all information stored on disk. When the computer is turned on, the user must supply a key to the encryption hardware. The information cannot be read meaningfully without this key, so even if the disk is stolen, the information on it will not be usable.

3. Integrity in Transmission: A typical technique for assuring integrity is to perform a checksum of the information being transmitted and transmit the checksum in encrypted form. Once the information and encrypted checksum are received, the information is again checksummed and compared to the transmitted checksum after decryption. If the checksums agree, there is a high probability that the message is unaltered.

4. Authentication of Identity: A typical algorithm for transforming any string into an encrypted password is designed so that it takes 10 or more msec/transformation to encode a string. By simple calculation, if only capital letters were allowed in a password, it would take .26 seconds to check all the one letter passwords, 6.76 seconds to check all the 2 letter passwords, 4570 seconds for the 4 letter passwords, and by the time we got to 8 letter passwords, it would take about 2*10**9 seconds (24169 days, over 66 years).

5. Credentialing Systems: Electronic credentials are designed to allow the credence of a claim to be verified electronically. Although no purely electronic credentialing systems are in widespread use at this time, many such systems are being integrated into the smart-card systems in widespread use in Europe. A smart-card is simply a credit-card shaped computer that performs cryptographic functions and stores secret information. When used in conjunction with other devices and systems, it allows a wide variety of cryptographic applications to be performed with relative ease of use to the consumer.

Chapter 4

Conclusion

As we toward a society where automated information resources are increased and cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The information security can be easily achieved by using Cryptography technique. DES is now considered to be insecure for some applications like banking system. there are also some analytical results which demonstrate theoretical weaknesses in the cipher. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable. By adding additional key, modified S-Box design, modifies function implementation and replacing the old XOR by a new operation as proposed by this thesis to give more robustness to DES algorithm and make it stronger against any kind of intruding. DES Encryption with two keys instead of one key already will increase the efficiency of cryptography. [**?**]

References

@articleCryptography, url="https://www.garykessler.net/library/crypto.html", year="2006"
@articleRanger, title="The undercover war on your internet secrets: How online surveillance cracked our trust in the web", year="2015", author:"Ranger, Steve"
@articleKahn, title="The Codebreakers", year="1967", author="Kahn, David"
@siteCrypto, url="https://dirkstrauss.com/cryptography-succinctly/"