

Essentials of Cryptography in Network Security

Dr. Adil Jamil Zaru

Abstract— The main aim of this paper is about how to protect information in digital form and to provide security services. However, a general overview of network security and cryptography is provided and various algorithms are discussed. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The common attacks on digital signature were reviewed. The first method was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Fiat-Shamir signature schemes, DSA and related signature schemes are two other methods reviewed.

Index Terms— malicious, intruder, promiscuous, repudiation, paranoid, hieroglyphs,.

I. INTRODUCTION

Now a days Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is through cryptography. This paper has two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography in use today.

II. PURPOSE OF CRYPTOGRAPHY

It is the science of writing in secret code and 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 hieroglyphs in an inscription. It is then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any trusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals:

- a) Secret key (or symmetric) cryptography
- b) public-key (or asymmetric) cryptography and
- c) Hash functions.

In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn be decrypted into usable plaintext. In many of the descriptions

below, two communicating parties will be referred to as Jimmy and Bobby; this is the nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. John is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party to the communication.

III. NETWORK SECURITY

It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas:

- a) Secrecy
- b) Authentication
- c) No repudiation and
- d) Integrity control

A. Secrecy

Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. No repudiation deals with signatures within the context of any application-to-application communication, there are some specific security requirements including: authentication.

Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.

Message Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

Non-repudiation: A mechanism to prove that the sender really sent this message.

B. Authentication

The process of proving one's identity. The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak. Both the sender and receiver need to confirm the identity of the other party involved in the communication - to confirm that the other party is indeed who or what they claim to be. If someone calls on the phone claiming to be your bank and asking for your account number, secret PIN, and account balances for verification purposes, would you give that information out over the phone? Hopefully not

C. Privacy/Confidentiality

Ensuring that no one can read the message except only the sender and intended receiver should be able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message be somehow encrypted (disguised data) so that an

intercepted message cannot be decrypted (understood) by an interceptor. This aspect of secrecy is probably the most commonly perceived meaning of the term "secure communication." Note, however, that this is not only a restricted definition of secure communication, but a rather restricted definition of secrecy as well.

D. Message Integrity

Assuring that the receiver received message has not been altered in any way from the original. Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission.

E. Non repudiation

Non-repudiation is a mechanism to prove that the sender really sent this message. It deals with signatures having established what we mean by secure communication; let us next consider exactly what is meant by an "insecure channel." What information does an intruder have access to, and what actions can be taken? Jimmy, the sender, wants to send data to Bobby, the receiver. In order to securely exchange data, while meeting the requirements of secrecy, authentication, and message integrity, Jimmy and Bobby will exchange both control messages and data messages (in much the same way that TCP senders and receivers exchange both control segments and data segments). All or some of these messages will typically be encrypted. A passive intruder can listen to and record the control and data messages on the channel; an active intruder can remove messages from the channel and/or itself address messages into the channel.

F. Cryptography

Cryptography comes from the Greek words for "secret writing." It has a long and colorful history going back thousands of years. Professionals make a distinction between ciphers and codes. A cipher is a

character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast, a code replaces one word with another word or symbol. Codes are not used anymore, although they have glorious history. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the ciphertext, is then transmitted, often by messenger or radio. We assume that the enemy, or intruder, hears and accurately copies down the complete cipher text. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the cipher text easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder). The art of breaking ciphers, called cryptanalysis, and the art of devising them (cryptography) is collectively known as cryptology.

III. TYPES OF CRYPTOGRAPHIC ALGORITHMS

For purposes of this paper cryptographic algorithms 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 types 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
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt"

Information

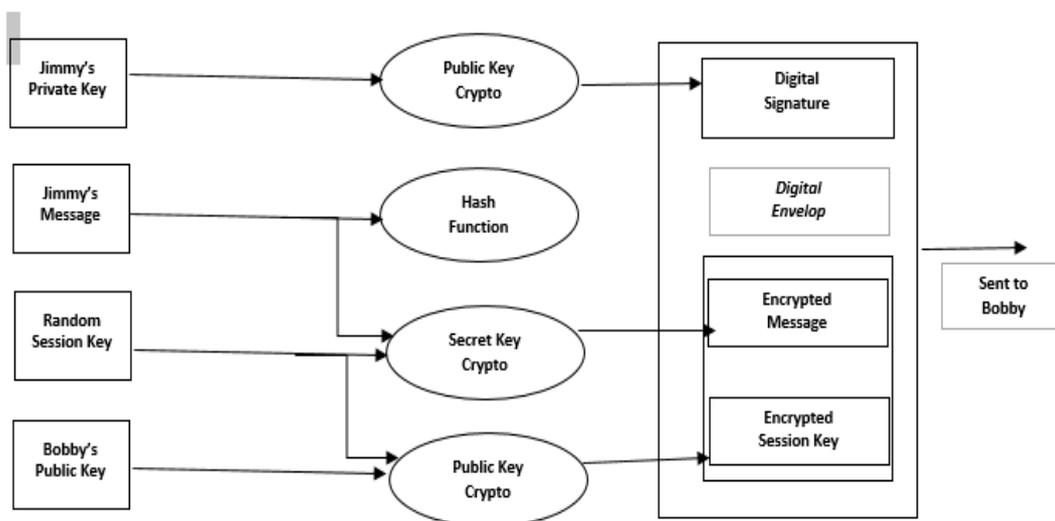


Figure -1

Two fundamental cryptographic principles

A. Redundancy

The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message.

Cryptographic principle 1: Message should contain some redundancy freshness.

Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds

later will be rejected as too old.

B. Symmetric Key Encryption Model

Beyond that, the security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm. We do not need to keep the algorithm secret, we need to keep only the secret key. The fact that the algorithm need not be kept secret means that manufacturers can and have developed low cost chip implementations of data encryption algorithms. These chips are widely available and incorporated into a number of products.

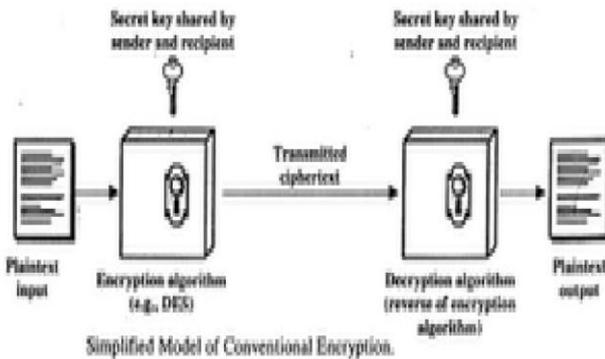


Figure 2

C. Substitution Ciphers

The simplest form of character – level encryption is substitution ciphering. In a substitution cipher each letter or group of letters is replaced by another letter or group of letters to disguise it. One of the oldest known ciphers is the Caesar cipher, attributed to Julius Caesar. In this method, a becomes D, b becomes E, c becomes F, and z becomes C.

For example, attack becomes DWDFN. The next improvement is to have each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter. For Example:

Plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

D. Transposition Ciphers

Substitution ciphers preserve the order of the plaintext symbols but disguise them. Transposition ciphers, in contrast, reorder the letters but do not disguise them. A common transposition cipher, the columnar transposition.

MEGABUCK
7 4 5 1 2 8 3 6

PLAIN TEXT: WELCOME TO ADIL,
JAMIL ZARU, JK.

CIPHER TEXT: CfHA OilKEeA8PALACRPT2LA

The cipher is keyed by a word or phrase not containing any repeated letters. In this example, MEGABUCK is the key. The purpose of the key is to number the columns, column 1 being under the key letter closest to the start of the alphabet, and so on. The plaintext is written horizontally, in rows, padded to fill the matrix if need be. The cipher text is read out by columns, starting with the column whose key letter is the

lowest.

Types of Cryptographic Attacks: Cryptographic attacks are designed to subvert the security of cryptographic algorithms, and they are used to attempt to decrypt data without prior access to a key. They are part of Cryptanalysis, which is the art of deciphering encrypted data. Cryptanalysis and Cryptography (the art of creating hidden writing, or ciphers) form the science of Cryptology.

E. Cryptographic Attack Methods

There are six related cryptographic attack methods, including three plaintext-based methods and three ciphertext-based methods:

Plaintext-Based Attacks	Known Plaintext	Chosen Plaintext	Adaptive Chosen Plaintext
Ciphertext-Based Attacks	Ciphertext Only	Chosen Ciphertext	Adaptive Chosen Ciphertext

Figure 3

These methods are used as the foundation of cryptographic attacks.

1) KNOWN PLAIN TEXT AND CIPHER TEXT – ONLY ATTACKS

A known plaintext attack is an attack where a cryptanalyst has access to a plaintext and the corresponding cipher text and seeks to discover a correlation between the two. A cipher text-only attack is an attack where a cryptanalyst has access to a cipher text but does not have access to corresponding plaintext. With simple ciphers, such as the Caesar cipher, frequency analysis can be used to break the cipher.

2) CHOSEN PLAIN TEXT AND CHOSEN CIPHER ATTACKS

A chosen plaintext attack is an attack where a cryptanalyst can encrypt a plaintext of his choosing and study the resulting cipher text. This is most common against asymmetric cryptography, where a cryptanalyst has access to a public key. A chosen cipher text attack is an attack where a cryptanalyst chooses a cipher text and attempts to find a matching plain text. This can be done with a decryption oracle (a machine that decrypts without exposing the key). This is also often performed on attacks versus public key encryption; it begins with a cipher text and searches for matching publicly-posted plain text data.

3) ADAPTIVE CHOSEN PLAIN TEXT AND ADAPTIVE CHOSEN CIPHER TEXT ATTACKS

In both adaptive attacks, a cryptanalyst chooses further plaintexts or cipher texts (adapts the attack) based on prior results.

a) Side Channel Attacks

Side channel attacks leverage additional information based on the physical implementation of a cryptographic algorithm, including the hardware used to encrypt or decrypt data. One example is the network based attack versus

Open SSL.

Open SSL uses two types of multiplication: one (called Karatsuba) for equal-sized words and normal multiplication for unequal-sized words. Karatsuba is faster, and the

difference in speed can be detected via a network using an SSL TCP/IP connection.

The type of multiplication in use leaks information to an attacker. Researchers at Stanford University were able to launch a side-channel timing attack to recover the 1024-bit

RSA key on an Open SSL 0.9.7 server. The attack required one million queries and took two hours.

b) Brute Force Attacks

A brute force attack systematically attempts every possible key. It is most often used in a known plaintext or cipher text only attack. Here is an example of a brute force attack on a 4-bit key:

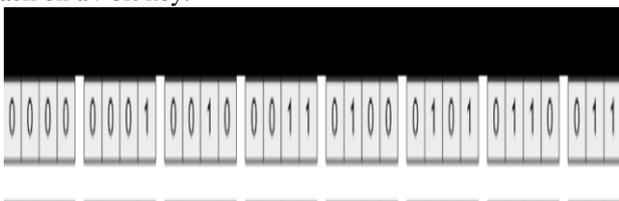


Figure 4

Given a finite key length and sufficient time, a brute force attack is always successful. Encryption algorithms can become susceptible to brute force attacks over time as CPU speeds increase. Single DES encryption has an effective key length of 56-bits, and any key can be cracked within days using specialized hardware, such as the Electronic Frontier Foundation's Deep Crack. Triple DES (168-bit key) was approved due to DES's weakness to brute force attacks, followed by the Advanced Encryption Standard (AES) in 2001.

c) Meet-in-the-Middle Attack

Meet-in-the-middle attacks can be used against cryptographic algorithms that use multiple keys for encryption. An example of a successful meet-in-the-middle attack is the attack versus Double DES.

4) Linear Cryptanalysis and Differential Cryptanalysis

Differential cryptanalysis and linear cryptanalysis are related attacks used primarily against iterative symmetric key block ciphers. The attacks can be combined, which is called differential linear cryptanalysis. A goal of strong encryption is to produce cipher texts that appear random where a small change in a plaintext results in a random change in the resulting cipher text.

a) Linear Cryptanalysis

Linear cryptanalysis is a known plaintext attack that requires access to large amounts of plaintext and cipher text pairs encrypted with an unknown key. It focuses on statistical analysis against one round of decryption on large amounts of cipher text. The cryptanalyst decrypts each cipher text using all possible sub keys for one round of

encryption and studies the resulting intermediate cipher text to seek the least random result. A sub key that produces the least random intermediate cipher for all cipher texts

becomes a candidate key (the most likely sub key).

b) Differential Cryptanalysis

Differential cryptanalysis is a chosen plaintext attack that seeks to discover relationship between cipher texts produced by two related plaintexts. It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm. A plaintext pair is created by applying a Boolean exclusive or (XOR) operation to a plain text. For example, XOR the repeating binary string 10000000 to the plaintext. This creates a small difference (hence the term differential cryptanalysis) between the two. The cryptanalyst then encrypts the plaintext and its XOR ed pair using all possible sub keys, and it seeks signs of non-randomness in each intermediate cipher text pair. The subkey that creates the least random pattern becomes the candidate key.

c) Birthday Attack

The birthday attack is an attack that can discover collisions in hashing algorithms. It is based on the Birthday Paradox, which states that if there are 23 people in a room, the odds are slightly greater than 50% that two will share the same birthday. Birthday and it is not the odds of sharing a birthday with a specific person. Jimmy is in a room with 23 the odds might appear counterintuitive. The key to understanding the attack is remembering that it is the odds of any two people (out of the 23) sharing a birthday and it is not the odds of sharing a birthday with a specific person. Jimmy is in a room with 23 people and has 22 chances to share a birthday with anyone else (there are 22 pairs of people). If she fails to match, she leaves, and Bobby has 21 chances to share a birthday with anyone else. If he fails to match, Carol has 20 chances, and so on. Twenty-two pairs, plus 21 pairs, plus 20... plus one pair equals 253 pairs. Each pair has a 1/365 chance of having a matching birthday, and the odds of a match cross 50% at 253 pairs. The birthday attack is most often used to attempt discover collisions in hash functions, such as MD5 or SHA1. IV. EARLY VS. MODERN CRYPTOGRAPHY Today's cryptography is vastly more complex than its predecessor. Unlike the original use of cryptography in its classical roots where it was implemented to conceal both diplomatic and military secrets from the enemy, the cryptography of today, even though it still has far-reaching military implications, has expanded its domain, and has been designed to provide a cost-effective means of securing and thus protecting large amounts of electronic data that is stored and communicated across corporate networks worldwide. Cryptography offers the means for protecting this data all the while preserving the privacy of critical personal financial, medical, and e-commerce data that might end up in the hands of those who shouldn't have access to it. There have been many advances in the area of modern cryptography. On January, 1977, the National Bureau of Standards (NBS) adopted a data encryption standard called the Data Encryption Standard (DES), which was a milestone in launching cryptography research and development into the modern age of computing technology. Moreover, cryptography found its way into the commercial arena when, on December, 1980, the same algorithm, DES, was adopted by the American National Standards Institute (ANSI). Following this milestone was yet another when a new concept was proposed to develop Public Key Cryptography (PKC), which is still undergoing research

development today(Levy, 2001). There are two forms of cryptosystems: symmetric and asymmetric. Symmetric cryptosystems involve the use of a single key known as the secret key to encrypt and decrypt data or messages. Asymmetric cryptosystems, on the other hand, use one key (the public key) to encrypt messages or data, and a second key (the secret key) to decipher or decrypt those messages or data. For this reason, asymmetric cryptosystems are also known as public key cryptosystems. The problem that symmetric cryptosystems have always faced is the lack of a secure means for the sharing of the secret key by the individuals who wish to secure their data or communications. Public key cryptosystems solve this problem through the use of cryptographic algorithms used to create the public key and the secret key, such as DES, which has already been mentioned, and a much stronger algorithm, RSA. The RSA algorithm is the most popular form of public key cryptosystem, which was developed by Ron Rivest, AdiShamir, and Leonard Adleman at the Massachusetts Institute of Technology in 1977 (Robinson, 2008). The RSA algorithm involves the process of generating the public key by multiplying two very large (100 digits or more) randomly chosen prime numbers, and then, by randomly choosing another very large number, called the encryption key. The public key would then consist of both the encryption key and the product of those two primes.

IV. CONCLUSION

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. This paper has described briefly about how cryptography works. The reader must beware, however because there are a number of ways to attack every one of these systems; cryptanalysis and attacks on cryptosystems, however, are well beyond the scope of this paper. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented. The strength of cryptography lies in the choice (and management) of the keys.

REFERENCES

- [1] Trappe, W., & Washington, L.C. (2006). Introduction to Cryptography with Coding Theory, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.
- [2] Denning, D.E. (1982). Cryptography and Data Security. Reading, MA: Addison-Wesley.
- [3] Ferguson, N., & Schneier, B. (2003). Practical Cryptography. New York: John Wiley & Sons.
- [4] Electronic Frontier Foundation. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. Sebastopol, CA: O'Reilly & Associates.
- [5] Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons.
- [6] Network Security Essential, William Stalling, Pearson Publications Ltd.