International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-4, Issue-5, May 2018 Pages 54-58

Essentials of Cryptography in Network Security

Dr. Adil Jamil Zaru

Abstract— **The main aim of this paper is about how to protect information indigital form and to provide security services. However, a general overview of network security and cryptography is provided andvarious algorithms are discussed. The purpose of a digital signature is to provide a meansfor an entity to bind its identity to a piece of information. Thecommon attacks on digital signature were reviewed. The firstmethod 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 aretwo other methods reviewed.**

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

I. INTRODUCTION

Now a days Internet provides essentialcommunication between tens of millions of people and isbeing increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.There are many aspects to security and manyapplications, ranging from secure commerce and payments to private communications and protecting passwords. Oneessential aspect for secure communications is throughcryptography. This paper has two major purposes. The firstis to define some of the terms and concepts behind basiccryptographic methods, and to offer a way to compare themyriad cryptographic schemes in use today. The second is toprovide some real examples of cryptography in use today..

II. PURPOSE OF CRYPTOGRAPY

It is the science of writing in secret code and is an ancient art, the first documented use of cryptography inwriting dates back to circa 1900 B.C. when an Egyptianscribe used non-standard hieroglyphs in an inscription. Itis then, that new forms of cryptography camesoon after the widespread development of computercommunications. In data and telecommunications,cryptography is necessary when communicating over anyentrusted medium, which includes just about anynetwork,particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used foruser authentication. There are, in general, three types ofcryptographic schemes typically used to accomplish thesegoals:

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

In all cases, theinitial unencrypted data is referred to as plaintext. It isencrypted into cipher text, which will in turn bedecrypted into usable plaintext.In many of the descriptions below, two communicating parties will be referred to as Jimmy and Bobby; this is thenomenclature in the crypto field and literature tomake it easier to identify the communicating parties. If thereis a third or fourth party to the communication, they will bereferred to as Carol and Dave. John is a malicious party,Eve is an eavesdropper, and Trent is a trusted third party tothe communication.

III. NETWORK SECURITY

It is concerned withpeople trying to access remote services that they are notauthorized to use. Most security problems are intentionallycaused by malicious people trying to gain some benefit, getattention, or to harm someone. Network security problemscan 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 withkeeping information out of the hands of unauthorized users.This is what usually comes to mind when people think aboutnetwork security. Authentication deals with determiningwhom you are talking to before revealingsensitive information or entering into a business deal. No repudiation deals with signatures within the context of anyapplication-to-application communication, there are somespecific security requirements including: authentication.

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

Message Integrity: Assuring the receiver that thereceived message has not been altered in any wayfrom the original.

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

B. Authentication

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

C. Privacy/Confidentiality

Ensuring that no one can read the message except onlythe sender and intended receiver should be able tounderstand the contents of the transmitted message. Becauseeavesdroppers may intercept the message, this necessarilyrequires that the message be somehow encrypted (disguisedata) so that an

First Author name, Department of Information Systems and Computer Science, Mahyail Aseer King Khalid University

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

D. Message Integrity

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

E. Non repudiation

Non-repudiation is amechanism to prove that the sender really sent this message. It deals with signatures havingestablished what we mean by secure communication; let usnext consider exactly what is meant by an "insecurechannel." What information does an intruder have access to,and what actions can beJimmy, the sender, wants to send data to Bobby, the receiver.In order to securely exchange data, while meeting therequirements of secrecy, authentication, and messageintegrity, Jimmy and Bobby will exchange both control messageand data messages (in much the same way that TCP sendersand receivers exchange both control segments and datasegments). All or some of these messages will typically beencrypted. A passive intruder can listen to and record thecontrol and data messages on the channel; an active intrudercan remove messages from the channel and/or itself addmessages into the channel.

F. Cryptography

Cryptography comes from the Greek words for "secretwriting." It has a long and colorful history going backthousands of years. Professionals make a distinction betweenciphers and codes. A cipher is a character-for-character orbit-for-bit transformation, without regard to the linguisticstructure of the message. In contrast, a code replaces oneword 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. Weassume that the enemy, or intruder, hears and accuratelycopies down the complete cipher text. However, unlike theintended recipient, he does not know what the decryptionkey is and so cannot decrypt the cipher text easily.Sometimes the intruder can not only listen to thecommunication channel (passive intruder) but can alsorecord messages and play them back later, inject his ownmessages, or modify legitimate messages before they get tothe receiver (active intruder). The art of breaking ciphers,called cryptanalysis, and the art devising them(cryptography) is collectively known as cryptology.

III. TYPES OF CROPTPGRAPHIC ALGORITHMS

For purposes of this paper cryptographic algorithms will becategorized based on the number of keys that are employedfor encryption and decryption, and further defined by theirapplication and use. The three types of algorithms that willbe discussed are

- Secret Key Cryptography (SKC): Uses a single keyfor both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematicaltransformation to irreversibly "encrypt"

Information

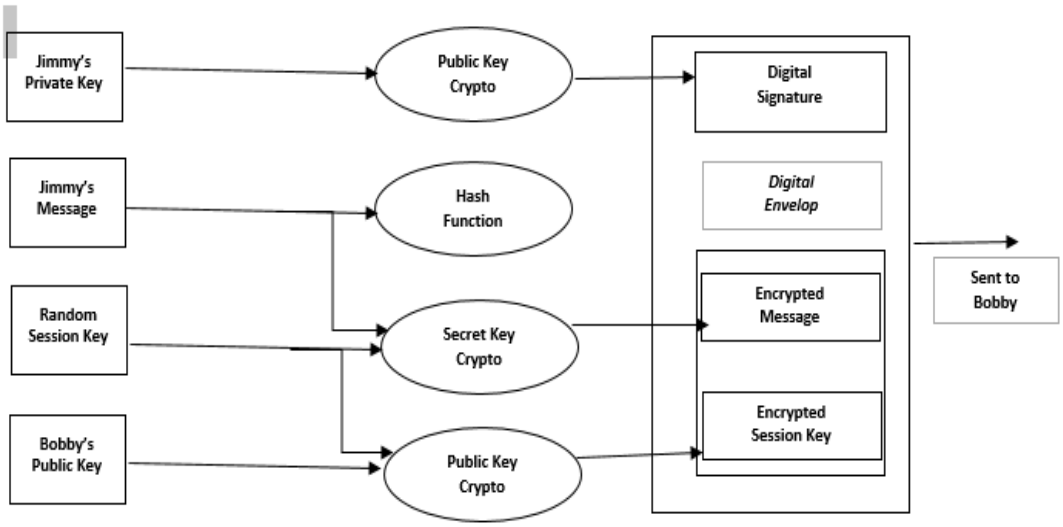

Figure -1

Two fundamental cryptographic principles

A. Redundancy

The first principle is that all encrypted messages mustcontain some redundancy, that is, information not needed tounderstand the message.

Cryptographic principle1: Message should contain someredundancy freshness.

Cryptographic principle 2: Some method is needed to foilreplay attacksOne such measure is including in everymessage 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 filterout duplicates. Messages older than 10 seconds can bethrown out, since any replays sent more than 10 seconds

laterwill be rejected as too old.

B. Symmetric Key Encryption Model

Beyond that, the security of conventional encryptiondepends on the secrecy of the key, not the secrecy of thealgorithm. We do not need to keep the algorithm secret, weneed to keep only the secret key. The fact that the algorithmneed not be kept secret means that manufactures can andhave developed low cost chip implementations of dataencryption algorithms. These chips are widely available andincorporated into a number of products.

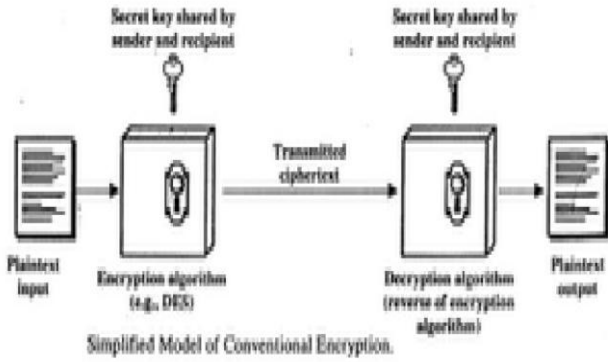

Figure 2

C. Substitution Ciphers

The simplest form of character – level encryption issubstitution ciphering. In a substitution cipher each letter orgroup of letters is replaced by another letter or group of

letters to disguise it. One of the oldest known ciphers is theCaesar cipher, attributed to Julius Caesar. In this method, abecomes D, b becomes E, c becomes F, and z becomes C.

For example, attack becomes DWWDFN.The next improvement is to have each of the symbols inthe plaintext, say, the 26 letters for simplicity, map ontosome 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 ZX C V B N M

D. Transposition Ciphers

Substitution ciphers preserve the order of the plaintextsymbols but disguise them. Transposition ciphers, incontrast, reorder the letters but do not disguise them depicts acommon transposition cipher, the columnar transposition.

M E G A B U C K

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 thekey. The purpose of the key is to number the columns, column 1 being under the key letter closest to the start of thealphabet, and so on. The plaintext is written horizontally, inrows, padded to fill the matrix if need be. The cipher text isread out by columns, starting with the column whose keyletter is the lowest.

Types of Cryptographic Attacks: Cryptographic attacksare designed to subvert the security of cryptographicalgorithms, and they are used to attempt to decrypt datawithout prior access to a key. They are part of Cryptanalysis, which is the art of deciphering encrypted data. Cryptanalysisand Cryptography (the art of creating hidden writing, orciphers) 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:

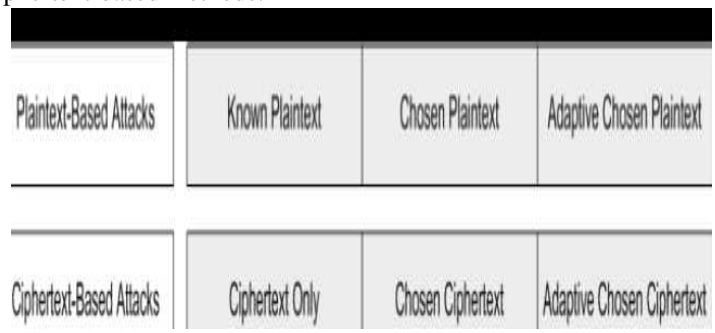

Figure 3

These methods are used as the foundation of cryptographicattacks.

1) KNOWN PLAIN TEXT AND CIPHER TEXT –ONLY ATTACKS

A known plaintext attack is an attack where acryptanalyst has access to a plaintext and the correspondingcipher text and seeks to discover a correlation between thetwo.A cipher text-only attack is an attack where a cryptanalysthas access to a cipher text but does not have access tocorresponding plaintext. With simple ciphers, such as theCaesar cipher, frequency analysis can be used to break thecipher.

2) CHOSEN PLAIN TEXT AND CHOSEN CIPHER ATTACKS

A chosen plaintext attack is an attack where acryptanalyst can encrypt a plaintext of his choosing andstudy the resulting cipher text. This is most common againstasymmetric cryptography, where a cryptanalyst has access toa public key.A chosen cipher text attack is an attack where acryptanalyst chooses a cipher text and attempts to find amatching plain text. This can be done with a decryptionoracle (a machine that decrypts without exposing the key).This is also often performed on attacks versus public keyencryption; it begins with a cipher text and searches formatching Publicly-posted plain text data.

3) ADAPTIVE CHOSEN PLAIN TEXT AND ADAPTIVE

CHOSEN CIPHER TEXT ATTACKS

In both adaptive attacks, a cryptanalyst chooses furtherplaintexts or cipher texts (adapts the attack) based on priorresults.

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 (calledKaratsuba) for equal-sized words and normal multiplicationfor unequal-sized words. Karatsuba is faster, and the

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

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

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

b) Brute Force Attacks

A brute force attack systematically attempts every possiblekey. It is most often used in a known plaintext or cipher textonlyattack. Here is an example of a brute force attack on a4-bit key:

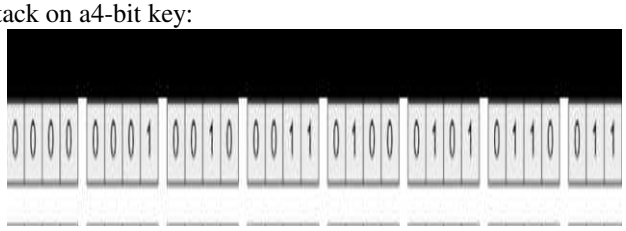

Figure 4

Given a finite key length and sufficient time, a brute forceattack is always successful. Encryption algorithms canbecome susceptible to brute force attacks over time as CPUspeeds increase. Single DES encryption has an effective keylength of 56-bits, and any key can be cracked within daysusing specialized hardware, such as the Electronic FrontierFoundation's Deep Crack. Triple DES (168-bit key) wasapproved due to DES's weakness to brute force attacks,followed by the Advanced Encryption Standard (AES) in2001.

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 cipher6 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 Oftwo 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-randomnessin 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 a1/365 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 CRYPTOGRAPHYToday's cryptography is vastly more complex than its predecessor. Unlike the original use of cryptography in itsclassical roots where it was implemented to conceal bothdiplomatic 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 beendesigned 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 ecommerce 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 thekeys.

REFERENCES

[1] Trappe, W., & Washington, L.C. (2006). Introduction toCryptography with Codin 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. NewYork: John Wiley & Sons.
[4] Electronic Frontier Foundation. (1998). Cracking DES: Secrets ofEncryption 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 Staling, Pearson PublicationsLtd.