International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cracking of Cryptographic Attack

Debosree Ghosh

Department of Computer Science and Engineering, Shree Ramkrishna Institute of Science and Technology
debosree_ghosh@yahoo.co.in;

ABSTRACT

Cryptography is the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks. This paper contains details about cryptography. Suppose that someone wants to send a message to a receiver, and wants to be sure that no-one else can read the message. However, there is the possibility that someone else opens the letter or hears the electronic communication. Cryptography depends on random numbers. These are hard for computers, which are decidedly non-random machines, to generate. Cryptography also depends on so-called "trapdoor functions", bits of mathematics that are easy to do in one direction but virtually impossible to reverse. One common method is based on the assumed difficulty of finding the prime factors of enormous numbers. So to prevent this issue many methodologies are used, which are discussed in this paper. How ASCII codes can be used in cryptography and Encryption by Listening to the Tiny Sounds made by Computer's CPU are also being discussed.

I. Introduction

Cryptography [14,15] deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications. In today's world of electronic commerce on the Internet, the need for secure communications is obviously crucial. Now encryption of electronic data is an essential part of modern life. It secures the financial networks that link the world's banks, protects credit cards, stops mobile-phone calls from being listened to, guards medical records and lawyers' letters to their clients.

Cryptographic technologies provide enterprises with the best mechanisms of protecting their information, without putting the business at risk by exposing it on the Net.

Suppose a company wants to transmit data over the telephone, but it is concerned that its phones may be tapped. All of its data is transmitted as four-digit integers. It has asked you to write a program that will encrypt its data so that the data may be transmitted more securely. Your script should read a four digit integer entered by the user in a prompt dialog and encrypt it as follows: Replace each digit by (the sum of that digit plus 7) modulus 10. Then swap the first digit with the third, and swap the second digit with the fourth. Then output XHTML text that displays the encrypted integer.

II. Background

1. Cryptography: Cryptography [14,15] enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. It is the Science of information security. It is closely related to the disciplines of cryptology and cryptanalysis.

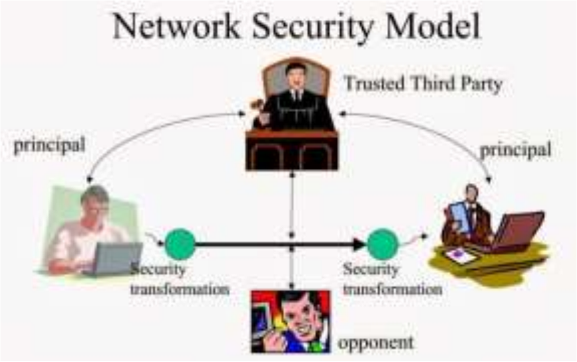


Figure - 1

2. Cryptology: It is the science of designing and breaking cryptosystem.

3. Cryptanalysis: The study of breaking cryptosystems is referred to as cryptanalysis.

4. Cryptosystem: It is a system for encryption and decryption of information.

5. Decryption: It is the process of taking encrypted data and rendering it readable for trusted users.

Cipher Text
Plain Text

6. Encryption: It is the process of taking data and modifying it so that it cannot be read by untrusted users.

Plain Text
Cipher Text

Note

Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

7. Plain Text: Plain text or a clear text is an intelligible message that is to be converted into an unintelligible (i.e encrypted) form.

8. Cipher Text: It is a message in encrypted form.

9. Cipher: It is the algorithm for performing encryption or decryption i.e a series of well defines steps that can be followed as a procedure.

Note

- A thread to a system in which an intruder can have access to only the cipher text is called a cipher text only attack.
- A thread to a system in which an intruder can have accessto both the cipher and considerable amount of corresponding plain text is said to be subject to a known plain text attack.

10. Key: For both encryption and decryption a key parameter is required whose secrecy is absolutely essential to the functioning of the entire process. Breaking a cryptographic system essential involves acquiring knowledge of key.

11. Private Key: A private key is known only to the owner or the owner's client program.

12. Public Key: A public key is distributed to any user (or to any client program) who requests it.

Note

The public and private key are related mathematically, someone could take another person's public key, perform complex mathematical calculation on it and extract the corresponding private key.

III. Different Methodology

- **Modern Cryptography**

1. Secret key or symmetric cryptography: It involves a private or secret key that was shared by the individuals involved in the transmission. The main problem with this type of cryptography is that how the owner of the key can securely transmit the key. Since the key is same for both encryption and decryption, the system referred to as the symmetric

Plain Text
Cipher Text
Plain Text

K is secret key

P is plaintext

C is cipher text

E is encryption function takes two parameters (K and P)

D is decryption function takes two parameters (K and C)

Using E function Alice encrypted the plaintext P with secret key K.

E (K, P) =C

Bob decrypted the cipher text C using D function.

D (K, C) =P

Symmetric cryptography has two branches, one deal with block cipher and second with stream cipher.

Example: - OTP (one time Pad or Password)

Note

In cryptography, a one-time pad[2,3] (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with random, secret key (or pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, and at least as long as the plaintext, and never reused in whole or in part, and kept completely secret, then the resulting cipher text will be impossible to decrypt or break.

2. Public key or asymmetric cryptography: It solves the problem by creating a set of two different keys for anyone needing to transmit encrypted information.

A precise mathematical relationship exists between the two keys, which together are called a key pain.

Plain Text
Cipher Text
Plain Text

PuK is public key

PvK is private key

P is plain text

C is cipher text

K is key (PuK or PvK

M is message (P or C)

E is encryption function takes two parameters (K and M)

D is decryption function takes two parameters (K and M)

Alice has published its public key to that any interested party can send confidential message which only Alice can decrypt.

Bob got the public key PuK and encrypted the plain message P using encryption function E to produce a secret message C.

E (PuK,P)=C

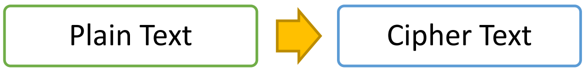
Bob transmitted this message over internet which is insecure communication channel. Bob need not to worry about security of his message because the message can be decrypted with only the private key in public-private key pair.

Alice got the message and decrypted with private key using D function to get the pain text.

D (PvK,C)=P.

Example: - Digital Signature.

3. Hash Function or one way cryptography: Hash functions have no key since the plaintext is not recoverable from the cipher text.



H is hash function

I is arbitrary input

h is hash value

H(I) = h

Using hash value h you can't compute the input I.

Let R be reverse-hash function.

R(h) ≠ I

Example: - Message authentication codes.

- **Computer Cryptography**

1. DES (Data Encryption Standard): DES[4,5] (the Data Encryption Standard) is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1.

It is a private key system.

Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. If we consider a triple length key to consist of three 56-bit keys K1, K2, K3 then encryption is as follows:

• Encrypt with K1

• Decrypt with K2

• Encrypt with K3

Decryption is the reverse process:

• Decrypt with K3

• Encrypt with K2

• Decrypt with K1

Setting K3 equal to K1 in these processes gives us a double length key K1, K2.

Setting K1, K2 and K3 all equal to K has the same effect as using a single-length (56-bit key). Thus it is possible for a system using triple-DES to be compatible with a system using single-DES

Example: - Bulk data Encryption.

2. RSA: RSA[4] is a public key algorithm invented by Rivest, Shamir and Adleman. The key used for encryption is different from (but related to) the key used for decryption.

The algorithm is based on modular exponentiation. Numbers e, d and N are chosen with the property that if A is a number less than N, then (Ae mod N)d mod N = A.

This means that you can encrypt A with e and decrypt using d. Conversely you can encrypt using d and decrypt using e (though doing it this way round is usually referred to as signing and verification).

• The pair of numbers (e,N) is known as the public key and can be published.

• The pair of numbers (d,N) is known as the private key and must be kept secret.

The number e is known as the public exponent, the number d is known as the private exponent, and N is known as the modulus. When talking of key lengths in connection with RSA, what is meant is the modulus length.

Example: - Digital signatures and for protecting DES keys.

3. MD5(Message Digest): MD5[4] is a hashing algorithm that takes a message of up to 264 bits and reduces it to a digest of 128 bits (16 bytes).

The algorithm is a development of the MD4 algorithm invented by Ronald Rivest and announced in 1990.

4. AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.

5. SHA-1: SHA-1[4] is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes).Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reason SHA-1 is recommended in preference to MD5.

6. HMAC: HMAC[4] is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

- **Classic Cryptography**

1. Transposition Cipher: It re-arranges the order of letter in a Message.

Example: - RITA IS A GOOD GIRL

ATRI IS A OGDO RLIG

2. Substitution Cipher: It re-arranges/systematically replaces letters or groups of letters.

Example: - FLY AT ONCE

GMZ BU PODF

3. Caesar Cipher: In it each letter in the plaintext was replaced by a letter, some fixed number of positions further down the alphabet.

Example: - ABCDEFGH → DEFGHABC

4. Polyalphabetic Cipher: It is any cipher based on substitution, using multiple substitution alphabets.

Example: - Vigenere Cipher (Encryption uses a key word, which controls letter substitution depending on which letter of the key word is used.)

5. Herodotus: Concealed a message inform of a tattoo on a slave's shaved head.

6. Steganography: Hiding even the existence of a message so as to keep it confidential.

Example: - Invisible Ink, Digital watermarks.

- **Other Cryptography**

1. Stream Cipher: Stream cipher [12] is a symmetric key cipher where plaintext digits are combined with a pseudorandom (process that appears to be random but is not) cipher digit stream (key stream).Alternative name is a state cipher, as the encryption of each digit is depended on the current state.

The key stream generator function produces keys K1, K2, K3 … which are XORed with plaintext P1, P2, P3 … to produce cipher text C1, C2, C3 …

C(i) = K(i) XOR P(i)

For decryption,

P(i) = K(i) XOR C(i)

RC4 is widely used stream cipher.

2. Block Cipher: Block Cipher[10] is a deterministic algorithm operating on fixed length of bits called blocks, with an unvarying transformation that is specific by a symmetric key.

It takes two inputs, 'n' bits of fixed length of blocks and a secret key and output is 'n' bits of cipher text.

P is fixed size n bits plaintext

K is secret key

E is encryption algorithm

D is decryption algorithm

C is fixed size n bits cipher text

E (P, K) = C

D(C, K) = P

3. Product Cipher: It combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis.

4. Feistel Cipher: In cryptography, a Feistel cipher [11] is a symmetric structure used in the construction of block ciphers. It is also commonly known as a Feistel network. The Feistel structure has the advantage that encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. The text being encrypted is split into two halves and two halves are swapped.

5. Iterated Cipher: An iterated block [10] cipher is one that encrypts a plaintext block by a process that has several rounds. In each round, the same transformation or round function is applied to the data using a sub-key. The set of sub-keys are usually derived from the user-provided secret key by a key schedule.

The number of rounds in an iterated cipher depends on the desired security level and the consequent trade-off with performance. In most cases, an increased number of rounds will improve the security offered by a block cipher, but for some ciphers the number of rounds required to achieve adequate security will be too large for the cipher to be practical or desirable

6. Visual cryptography: Visual cryptography [1] is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

7. Trapdoor function: It is a one-way function which is easy to compute in one direction and hard to compute in reverse direction. However with a secret key which is known as trapdoor it

is easy to compute in reverse direction.

IV. Cryptography used in The Real World

1. Passphrase: A passphrase is a longer version of a password, and in theory, a more secure one. Typically composed of multiple words, a passphrase is more secure against standard dictionary attacks, wherein the attacker tries all the words in the dictionary in an attempt to determine your password.

The best passphrases are relatively long and complex and contain a combination of upper and lowercase letters, numeric and punctuation characters.

2. Key Splitting[9]: It is wise to split the key among multiple people in such a way that more than one or two people must present a piece of the key in order to reconstitute it to a usable condition. If too few pieces of the key are available, then the key is unusable.

Examples: - Split a key into three pieces and require two of them to reconstitute the key, or split it into two pieces and require both pieces. If a secure network connection is used during the reconstitution process, the key's shareholders need not be physically present in order to rejoin the key.

3. Digital Certificate: A digital certificate is data that functions much like a physical certificate. A digital certificate is information included with a person's public key that helps others verify that a key is genuine or *valid.* Digital certificates are used to thwart attempts to substitute one person's key for another.

A digital certificate consists of three things:

- A public key.
- Certificate information. ("Identity" information about the user, such as name, user ID, and so on.)
- One or more digital signatures.

The purpose of the digital signature on a certificate is to state that the certificate information has been attested to by some other person or entity.

4. Digital Signature: Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity.

5. Security Token: A security token [6] (or sometimes a hardware token, authentication token, USB token, cryptographic token, software token, virtual token, or key fob) may be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens.

Security tokens are used to prove one's identity electronically.

6. Key Fob: A key fob [6,7] is a generally decorative and at times useful item many people often carry with their keys, on a ring or a chain, for ease of tactile identification, to provide a better grip, or to make a personal statement. It is a small hardware device with built in authentication mechanisms.

7. Brute Force Cracking: Brute Force Cracking [13] is a trial and error method used to decode encrypted data through exhaustive effort rather than employing intellectual strategies.

A birthday attack is a name used to refer to a class of brute-force attacks. It gets its name from the surprising result that the probability that two or more people in a group of 23 share the same birthday is greater than 1/2; such a result is called a birthday paradox.

8. Salt: In password protection this is a random string of data used to modify a password hash.

9. Electronic Code Book: This is a mode of operation for a block cipher, with the characteristics that each possible block of plain text has a defined corresponding cipher text value and vice versa.

10. Message Authentication Code (MAC): Message authentication code is value or checksum attached with original message to provide authenticity and integrity of data. MAC is calculated using a hash function and a secret key.

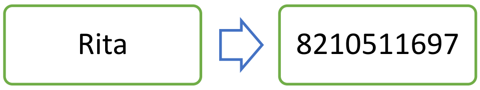
V. ASCII Effect in Cryptography

The American Standard Code for Information Interchange is a character-encoding scheme originally based on the English alphabet that encodes 128 specified characters - the numbers 0-9, the letters a-z, and A-Z, some basic punctuation symbols, some control codes that originated with Teletype machines, and a blank space - into the 7-bit binary integers.

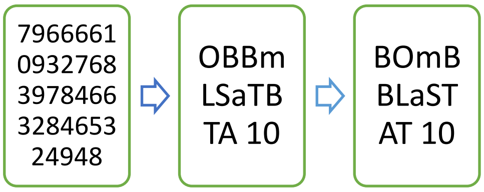
In it each letter in the plaintext was replaced by it's ASCII value.

Proof:-

1.



2.



VI. Practical Attack

Not only must the work and computational resources required by the cryptanalyst be reasonable, but the amount and type of data required for the attack to be successful must also be taken into account.

A chosen plaintext or chosen cipher text attack gives the cryptanalyst the greatest freedom in analyzing a cipher. The cryptanalyst chooses the plaintext to be encrypted and analyzes the plaintext together with the resultant cipher text to derive the secret key. Such attacks will, in many circumstances, be difficult to mount but they should not be discounted. As Merkle and Hellman have remarked [MH81], a chosen text attack can in some ways be viewed as a "certification weakness" in a cryptosystem.

A known plaintext attack is more useful to the cryptanalyst than a chosen plaintext attack (with the same amount of data) since the cryptanalyst now requires a certain numbers of plaintexts and their corresponding cipher texts without specifying the values of the plaintexts. This type of information is presumably easier to collect.

The most practical attack, but perhaps the most difficult to actually discover, is a cipher text-only attack. In such an attack, the cryptanalyst merely intercepts a number of encrypted messages and subsequent analysis somehow reveals the key used for encryption. Note that some knowledge of the statistical distribution of the plaintext is required for a cipher text-only attack to succeed.

An added level of sophistication to the chosen text attacks is to make them adaptive. By this we mean that the cryptanalyst has the additional power to choose the text that is to be encrypted or decrypted after seeing the results of previous requests.

VII. Encryption by Listening to the Tiny Sounds made by Computer's CPU

One of the most secure encryption algorithms is 4096-bit RSA[8], here by listening with a *microphone* to a computer as it decrypts some encrypted data. The attack is fairly simple and can be carried out with rudimentary hardware. The repercussions for the average computer user are minimal, but if you're a secret agent, power user, or some other kind of encryption-using miscreant, you may want to reach for the Rammstein when decrypting your data. This method is called side channel. A side channel is an attack vector that is non-direct and unconventional, and thus hasn't been properly secured.

For example, your pass code prevents me from directly attacking your phone — but if I could work out your pass code by looking at the greasy smudges on your screen, that would be a side channel attack. In this case, the security researchers listen to the high-pitched (10 to 150 KHz) sounds produced by your computer as it decrypts data.

If you are able to listen for telltale signs that the CPU was decrypting some data, and then listening to the following stream of sounds to divine the decryption key. The same attack would not work on different cryptosystems or different encryption software, we have to start back at the beginning and work out all of the tell-tale sounds from scratch. If you want to keep your data secure, you only really have two viable options: Heavy-duty encryption, physical security, and ideally both at the same time. If an attacker can't get physically close to your data, it instantly becomes much harder to steal it.

VIII. Conclusion

A attacker needs to make only one reliable correlation in order to continue guessing a password or private key. For practical attack the amount and type of data required for the attack should be taken into account. Proper use of ASCII code can help us to decode the encrypted message. We can decrypt data by listening the sound of CPU.

References

[1] O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. Optics Letters, Vol. 12, Issue 6, pp. 377–379 (1987).

[2] "The only unbreakable cryptosystem known—the Vernam cipher". Pro-technix.com. Retrieved 2014-03-17.

[3] "One-Time Pad (OTP)". Cryptomuseum.com. Retrieved 2014-03-17.

[4] http://www.cryptographyworld.com/index.htm.

[5]http://en.wikipedia.org/wiki/Data_Encryption_Standard.

[6] de Borde, Duncan (2007-06-28). "Two-factor authentication". Siemens Insight Consulting. Retrieved 2009-01-14.

[7] Largest Collection of Keychains". Guinness World Records. Retrieved 3 April 2011.

[8] RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis , December 18, 2013.

[9] http://www.pgpi.org/doc/pgpintro.

[10] Chakraborty, D. & Rodriguez-Henriquez F. (2008). "Block Cipher Modes of Operation from a Hardware Implementation Perspective". In Koç, Çetin K. Cryptographic Engineering. Springer. p. 321. ISBN 9780387718163.

[11] Luby, Michael; Rackoff, Charles (April 1988), "How to Construct Pseudorandom Permutations from Pseudorandom Functions", SIAM Journal on Computing 17 (2): 373–386.

[12] Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995.

[13] Paar, Christof; Pelzl, Jan; Preneel, Bart (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*.

[14] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science 1. Elsevier.