

CRYPTOGRAPHIC CONCEPTS

REVIEW OF CRYPTOGRAPHIC IMPLEMENTATIONS ASSIGNMENT



Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Unit Code : CSI2108

Name of Lecturer: Dr Liau Vui Kieu

Campus: PSB Academy, Singapore

Due Date: 06th April 2020

Contents

[Introduction 2](#_Toc37012687)

[Symmetric Encryption 2](#_Toc37012688)

[Symmetric encryption types 2](#_Toc37012689)

[Symmetric encryption algorithms examples 3](#_Toc37012690)

[Applications 3](#_Toc37012691)

[Advantages and Disadvantages 3](#_Toc37012692)

[Asymmetric encryption 4](#_Toc37012693)

[Asymmetric encryption algorithms examples 4](#_Toc37012694)

[Applications 4](#_Toc37012695)

[Advantages and Disadvantages 5](#_Toc37012696)

[Significant differences between symmetric and asymmetric encryption 5](#_Toc37012697)

[Cryptography attacks 6](#_Toc37012698)

[Ciphertext – only 6](#_Toc37012699)

[Brute force attack 6](#_Toc37012700)

[Birthday attack 6](#_Toc37012701)

[Man in the Middle attack (MitM) 7](#_Toc37012702)

[Social Engineering 8](#_Toc37012703)

[Conclusion 9](#_Toc37012704)

[References 9](#_Toc37012705)

# Introduction

In the current computer era, technology grows and becoming advance day by day. Everyday new technology and innovations are coming out that helps for better improvement. And for this emerging technology information security helps to ensure that the technology is safe. In information, security cryptography places an important role. Cryptography is a measure that helps to encode the message and make it as unreadable without proper authentication measures. The process of cryptography involves two things one is encryption and second one is decryption. Encryption is a process of converting a plain text to unreadable form which is known as cipher text. Decryption is a reverse process of converting the cipher text into a readable format after a proper validation. Cryptography ensures the first principle of CIA i.e. Confidentiality. There are various algorithms are being used in cryptography and this paper reviews the well-known encryptions symmetric and asymmetric encryption. Also, this paper explains the attacks that target the cryptography.

# Symmetric Encryption

The symmetric encryption method is also known as a single key and secret key encryption mechanism (Paar & Pelzl, 2011). In symmetric encryption (Cobb, 2004) only one key will be used for both the encryption and decryption processes and in this the encrypted data cannot be decrypted by anyone who has no relevant decryption key. Only the intended party can decrypt with the relevant key. The same key used in the symmetric encryption can be a password, code that both parties involved know. Apart from that, the key can be a string or combination of letters and numbers that are generated by the secure random generator. The formula used for symmetric key algorithm is N= n\*(n-1)/2, (N number of keys needed, n is the number of people)

## Symmetric encryption types

Symmetric encryption typically consists of two types of algorithms they are block algorithm and stream algorithm (Teach Computer Science, n.d.) .

**Block algorithm –** In block algorithm, the encrypted data will be retained from the system’s memory. Also, the specified lengths of bits are encrypted with the use of a common secret key in electronic data blocks.

**Stream algorithm –** In-stream algorithm the encrypted data will be retained from a stream rather than retrieving from the system’s memory.

## Symmetric encryption algorithms examples

In the cryptography domain, several algorithms are based on the symmetric encryption method. Some of the well-known symmetric encryption-based algorithms are (Sangeeta, 2017),

* DES (Data encryption standard)
* AES (Advanced encryption standard)
* TDEA or Triple DEA (Triple Data encryption algorithm)
* Blowfish

## Applications

The symmetric algorithm is being used multiple applications, especially it is being used for encrypting a large amount of data such as databases the reason is this algorithm is fast and efficient (Achuthshankar & Achuthshankar, 2015). Some of the applications that are using the symmetric algorithm are (Peter & Dawn, 2019) ,

* Payment applications like transactions using credit and debit cards to avoid identity theft
* In hashing symmetric algorithm can be used to generate random numbers/values.

## Advantages and Disadvantages

Some of the advantage and disadvantages of asymmetric as follows (Jessica, 2001),

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| If the key remains secret the authentication maintained in this is high | Since a single key is used the key has to be changed frequently but the process will not be feasible in large groups |
| Fast and efficient so can even the huge volume of data very quickly without any issues | Key distribution is complicated especially when exchanging in large size groups |
| Involvement of central authority is not required | If the number of users increases then the number of keys also increases which causes an impact in key maintenance. |

# Asymmetric encryption

Asymmetric encryption is also known as public-key encryption. The fundamental methodology asymmetric encryption is (Delfs & Knebl, 2011), the key will be separated into two parts as a private key and public key. And the public key will be made available for the public to use it for encryption and the private key will be kept as a secret with the relevant holder. So, party with the public key can encrypt the information which provides confidentiality and then the party with the appropriate private key can decrypt it. The primary purpose of this asymmetric encryption method is to establish a secure key distribution. The formula for asymmetric encryption is (N=2\*n) (N is the number of keys required; n is the number of people). Furthermore, asymmetric encryption used for authentication, secret key exchanges, and digital signatures.

## Asymmetric encryption algorithms examples

In the cryptography domain, several algorithms are based on the asymmetric encryption method. Some of the well-known asymmetric encryption-based algorithms are (Suguna & Manjupriya, 2016),

* Diffie-Hellman key exchanges
* RSA
* Elgamal cryptosystem
* Elliptic curve cryptography
* Digital signature

## Applications

A well-known application that is using the asymmetric algorithm is WhatsApp. According to WhatsApp security whitepaper (WhatsApp, 2017), the end-to-end encryption feature in WhatsApp basically generates a public key in the WhatsApp server whenever a user registers their device then the user device will be allocated with their relevant private key. Also, the private key for the user doesn’t get stored in the WhatsApp server. Also, the AES256 is used for encryption whenever a chat initiated between two users and HMAC- SHA256 is used for authentication.

Apart from secure communications, asymmetric encryption is being used in applications like digital signatures, application-level communications (layer seven in the OSI model).

## Advantages and Disadvantages

Some of the advantage and disadvantages of asymmetric as follows (Jessica, 2001),

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| The number of keys requires here is less and key management will become easy | Not all the algorithms are simultaneously safe and can be applied practically. |
| Distribution is simply because anyone can share anyone’s public key | The asymmetric encryption method is very slow and extremely time-consuming. |

# Significant differences between symmetric and asymmetric encryption

The following table consists of the key difference between both encryption systems (Chapple, Gibson & Stewart, 2018),

|  |  |  |
| --- | --- | --- |
| **Characteristic** | **Symmetric** | **Asymmetric** |
| Performance | Rapid because the algorithm is less complex | Since the algorithm is quite complex it is time-consuming |
| Key | Only one key involved throughout the process | Two keys involved. One party will have the public key of another party and another party will have the concerned private key |
| Exchange process | Depends upon out-of-band security mechanism | Since the public key is available to anyone with no complexities in the exchange process. |
| Service provided | Focuses on confidentiality | Primarily focuses on authentication and renounce |
| Usage | Bulk encryption like databases | The digital signature, key distributions, and secure communications. |

# Cryptography attacks

In cyber security all the technologies have their own security threats. The same applies to cryptography also. There various attacks available that targets the cryptography domain. The following five attacks are just few examples of them.

## Ciphertext – only

Ciphertext -only attack is one of the notable attacks that has success rate even against the modern ciphers. Researches describes the attack as follows (Chapple, Gibson & Stewart, 2018), in this specific attack, the attacker must access only the large quantity of encrypted messages. Also, the attacks would have no knowledge about which is plaintext, or which is the secret key. The aim is to either retrieves as many plain text messages as possible or to guess the secret key. Once, discovering the encryption key, its possible for the attacker to crack all the other cipher texts that are made by the same key.

## Brute force attack

In general, brute force attack (Kaspersky, n.d.) is a method of cracking the password by using all the possible keys in the method of trial and error approach. It is one of the oldest password cracking method but still an efficient one.

This brute force method can be applied to cryptography also. The approach describes as follows (Ben, 2019), if the key for an encryption is 8-bit in length then the possible number of keys are 28 which is 256. So, if the attacker knows what kind of algorithm that the ciphertext follows they it will consume very less amount of time for crack that 8 bits key.

Though, it is a well-known attack method the efficiency is totally depends upon the key length and the algorithm used. Because if the key length is increases then the number of possible key combination also increases which results in time consumption. Blocking the user after a amount of login attempts will act as an efficient countermeasure for this.

## Birthday attack

Birthday attack is a kind of brute force attack. In this instead of cracking the cipher text it aims to crack the hash function. The fundamental of this attack is to exploit the mathematical behind the birthday problem that comes under in the theory of probability. The success of this attack is fully based on likelihood of the Collison between the strings. The mathematical behind this attack is described as follows (Yatharth, n.d.),

If a class room has 23 students the possibility of two students having the same date of birth would be 0.50 and it the number of students increases to 30 the the probability also increases to 0.70. This incident is known as birthday paradox. The mathematical used for 30 students present in a class is 365!/((365-n)! \* 365n)

This same applies to cryptography also. In general has function known as H is a conversion that acquire the input ‘m’ of a variable size and return back a string of fixed length called as hash value thus (h=H(m)). So if we apply the formula p(n; H) = 1 - ( (365-1)/365) \* (365-2)/365) \* ...(365-n+1/365)) here then the output would be p(n; H) = e-n(n-1)/(2H) = e-n2/(2H). So if the attacker managed to find the two diverse inputs that provides the similar hash value it will be considered as collision.

## Man in the Middle attack (MitM)

In general, MitM attacks are aimed to intercept the electronic communications in order to sniff on transmissions in an attack against the confidentiality then process further to attack on integrity. MitM attack in cryptography describes as follows (Chris, n.d.),

The intruder first makes two secret keys. The he uses the first key to state the initiation of conversation. The response obtained is encrypted but still it can be easily decrypted by the intruder since he knows the secret key. Then once again he encrypts the message but this time using the second key. The user then send the encrypted message back to the second side. Instead, after receiving the response from the other side, the message is decrypted, read, and encrypted again by the first key and sent back to the initiation stage by following the method the intruder can obtain a huge amount of information about the entire flow and can even impersonate as an approved user successfully and can gain access.

A good mutual authentication mechanism must be used to protect against this attack before the transmission of sensitive data begins. The other kind of security is to use existing public keys, which can be accessed from for example, existing databased, instead of using any encryption key obtained from one side of the communication.

## Social Engineering

Social engineering is an attack method that hugely depends upon human activity and frequently requires the exploitation of people to evade standard security protocols and practices in order to gain access to systems, networks, or infrastructure. The primary motive can be anything such as financial gain and so on (Margaret, 2018).

Threat actors use social manipulation tactics to hide their real identity and motivations and to portray themselves as a credible source of knowledge or individuals. The purpose is to control, exploit or trick users into giving up privileged information or access to an organization. Most social engineering successes simply depend on people's ability to be supportive (Oriyano, 2016).

For example (Oriyano, 2016), the attacker may claim to be a co- with emergency issue needing access to additional network resources. Social engineering is a common technique for hackers as it is often easier to exploit the vulnerabilities of users than to locate a network or software flaw.

The typical social engineering process as follow (Oriyano, 2016) ,

The first process is information gathering, it means that the intruder must know as much about the target or the business as possible. The second step is to prepare the attack, which is the planning of when to execute the attack against the target. Third stage is gathering the requirements such as software, computer programs that the intruder required to execute the attack against the target. The final (fourth) step is to execute the attack. In this stage the attacker will execute the attack against his target using the knowledge the gained in the first stage i.e. information gathering.

The typical attack methods are using phishing, vishing, taking advantage of human feelings such as fear, trust, and desire to help.

# Conclusion

As the technology grows the security threats also grows at the same time this applies to cryptography domain also. Since, in cyber security the threats cannot be eliminated completely in a single attempt emerging researches such as quantum cryptography will increase the level of security and protection.

# References

Achuthshankar, A., & Achuthshankar, A. (2015). A novel symmetric cryptography algorithm for fast and secure encryption. *2015 IEEE 9Th International Conference On Intelligent Systems And Control (ISCO)*. doi: 10.1109/isco.2015.7282273

Ben, H. (2019). Cryptographic Attacks: A Guide for the Perplexed - Check Point Research. Retrieved from <https://research.checkpoint.com/2019/cryptographic-attacks-a-guide-for-the-perplexed/>

Chapple, M., Gibson, D., & Stewart, J. (2018). *CISSP*. Sybex.

Chris, K. Crypto-IT. Retrieved from <http://www.crypto-it.net/eng/attacks/man-in-the-middle.html>

Cobb, C. (2004). *Cryptography for dummies*. Hoboken, N.J.: Wiley Pub.

Delfs, H., & Knebl, H. (2011). *Introduction to cryptography* (2nd ed.). Berlin: Springer.

Jessica, B. (2001). *SANS Institute Information Security Reading Room*. SANS. Retrieved from <https://www.sans.org/reading-room/whitepapers/vpns/pgp-hybrid-solution-717>

Kaspersky. What Is a Brute Force Attack? | Kaspersky. Retrieved from <https://www.kaspersky.com/resource-center/definitions/brute-force-attack>

Margaret, R. (2018). What is social engineering? - Definition from WhatIs.com. Retrieved from <https://searchsecurity.techtarget.com/definition/social-engineering>

Oriyano, S. (2016). *CEHv9: Certified Ethical Hacker Version 9 Study Guide*. John Wiley & Sons.

Paar, C., & Pelzl, J. (2011). *Understanding cryptography*. Berlin: Springer.

Peter, S., & Dawn, M. (2019). Symmetric Key Encryption - why, where and how it’s used in banking. Retrieved from <https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking>

Sangeeta. (2017). A Review on Symmetric Key Cryptography Algorithms. *International Journal Of Advanced Research In Computer Science*, *8*(4).

Suguna, S., & Manjupriya, R. (2016). A STUDY ON SYMMETRIC AND ASYMMETRIC KEY ENCRYPTION ALGORITHMS. *International Research Journal Of Engineering And Technology (IRJET)*, *03*(04). Retrieved from <https://www.irjet.net/archives/V3/i4/IRJET-V3I407.pdf>

Teach Computer Science. Symmetric Encryption | Types, Examples & Facts. Retrieved from https://teachcomputerscience.com/symmetric-encryption/

WhatsApp. (2017). *WhatsApp Encryption Overview Technical white paper*. Retrieved from <https://scontent.whatsapp.net/v/t61.22868-34/68135620_760356657751682_6212997528851833559_n.pdf/WhatsApp-Security-Whitepaper.pdf?_nc_sid=41cc27&_nc_ohc=_aIrOSJUBUQAX-IU30t&_nc_ht=scontent.whatsapp.net&oh=daae8787c2a39a39fc2832daa0eb48bc&oe=5E8A48D3>

Yatharth, S. Birthday attack in Cryptography - GeeksforGeeks. Retrieved from <https://www.geeksforgeeks.org/birthday-attack-in-cryptography/>