Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 8-11 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CRYPTOGRAPHY USE IN EVERYDAY LIFE

Niko salukvadze - mtsignobart uxucesi
Lizi Gogitidze - 51 public school
Giorigi Adamia - 52 public school

ABSTRACT: Cryptography plays a very important role in our everyday lives. Cryptography is used to transfer funds and data safety. It encrypts what we send so it can't be seen by anyone, other than the person we send it to or changed by a middleman. And thanks to the advances in cryptography, today we can send whatever want, without worrying about hackers getting this information. This article discusses how our information is encrypted and how secure this encryption method is.

KEYWORDS: *cryptography, cyber information, encrypted*

Introduction

In today's article, we talk about cryptography use in everyday life. Many people haven't heard anything about this word so they don't know how often cryptography is used in the 21st century. We can't take our phones as an example, because we store our most personal information on them they are very protected.

What is cryptography? what are the Different encryption methods? What is hashing? What is crypto analysis? How is cryptography used in everyday life?

The word cryptography comes from the greek word Kryptos, meaning hidden. Crypt means hidden, and the suffix -graphy stands for writing. It also is the science of hiding information. Cryptography is closely connected to mathematics and computer science. In everyday life, we see the use of cryptography in credit cards, transfers, passwords, and more. cryptography today is a normal profession that has sub-professions. Such as cryptoanalysis.

Cryptography and computer science are closely connected still both professions are quite demanded, both are very popular, and highly paid jobs but cryptography is more underrated.

Encryption methods and what they're used in

There are two different types of encryptions, symmetric and asymmetric. both have their advantages and disadvantages. Symmetric encryption works by giving the sender and the receiver a Secret Key this key is used to turn plaintext into ciphertext then this ciphertext is sent and the person that receives it uses the same key to decipher it back into plain text. This method's advantages are that symmetric encryption is fast and efficient when it comes to large files. Symmetric encryption is commonly used in Payment applications, such as card transactions where PII needs to be protected to prevent identity theft or fraudulent charges. Validations to confirm that the sender of a message is who he claims to be. Random number generation or hashing. The disadvantage to symmetric encryption is keeping the key secret. If a hacker gets this key all of the information that u send will be available to him. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.[1,2]

Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key. If the public key is used for encryption, then the related private key is used for decryption. if the private key is used for encryption, then the related public key is used for decryption. Although asymmetric encryption is much safer than symmetric it has many disadvantages such as: being slower, if the private key is lost u can't decrypt anything sent to you, public keys aren't authenticated, so no one can ensure a public key belongs to a specific person. Asymmetric encryption is used in key exchange, email security, web security, and other encryption systems that require key exchange over the public network such as SSL/TLS, SSH, and HTTPS

Hashing

Hashing is the process of transforming a given key or a string of characters into another value. this usually is represented by a shorter, value or key that represents and makes it easier to find the original string. A hash function generates new values using a mathematical hashing algorithm, known as a hash value or simply a hash. A good hash always uses a one-way hashing algorithm to prevent the hash from being turned into the original key. A hashing algorithm is a mathematical function that garbles data and makes it unreadable. Hashing is commonly used for Data indexing and retrieval, digital signatures, Encryption, and others.

the main difference between hashing and two other forms of data encryption is that once data is encrypted, it cannot be decrypted. This ensures that even if a hacker gets his hands on a hash, it will be useless since he cannot decrypt the contents of the message. Message Digest 5 and Secure Hashing Algorithm are two widely used hashing algorithms.

Hashing also has its disadvantage, for example, Hash is inefficient when there are many collisions it doesn't allow null values and hash collisions are practically not avoided for a large set of possible keys[5]

How SSL/HTTPS works

HTTPS(Hypertext Transfer Protocol Secure) secures communication and data between a user's web browser and a website. it appears in your URL when the website is secured by an SSL certificate.SSL(Secure Sockets Layer) is a bit of code on your web server that provides security for online communications.HTTPS uses an encryption protocol to encrypt communications. this protocol is called TLS(transport layer).HTTPS uses an asymmetric public key infrastructure to secure communications [3,4] .

Cryptoanalysis

Cryptoanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information. cryptoanalysis explores the weaknesses of the underlying mathematics of cryptographic systems but it includes looking for weaknesses in implementation, such as side-channel attacks or weak entropy inputs [5]. Side-channel attacks (SCAs) aim at extracting secrets from a chip or a system, through the measurement and analysis of physical parameters. Examples of these parameters are supply current, execution time, and electromagnetic emission. These attacks pose a serious threat to modules that integrate cryptographic systems, side-channel analysis techniques have proven successful in breaking encryptions and extracting the secret keys [6].

Money transfers

A lot of banks use ATMs because they are convenient and safe for taking money out of your bank account. And because their so widely used, the process of taking money out or putting it in needs to be encrypted. This encryption is known as Hardware Security Module Encryption(HSM). It protects our PIN confidentiality and other personal information, which exists on our credit or debit cards [7]. This system also ensures that cyber-criminals can't reach our PINs while the transaction is still active or when you use the ATM.

Conclusion

All in all, cryptography is a powerful tool today used for protecting our private information from hackers. We use it in our daily activities every time we send messages to transfer funds or transfer data, by using asymmetric or symmetric encryption our data is turned into cyphertext that cyber-criminals can't decipher without a special key. The most commonly used symmetric algorithm is AES-128 which is nearly impossible to decipher without a key. Even though modern encryption methods are really useful and convenient if not set up properly cyber criminals can decipher the information we send. And if the person loses their secret key somehow deciphering texts sent to them will be impossible to decipher.

Acknowledgement: This work was supported by Shota Rustaveli National Science Foundation of Georgia [SPG-22-218]

REFERENCE

1..Akkar, ML., Giraud, C. (2001). An Implementation of DES and AES, Secure against Some Attacks. In: Koç, Ç.K., Naccache, D., Paar, C. (eds) Cryptographic Hardware and Embedded Systems — CHES 2001. CHES 2001. Lecture Notes in Computer Science, vol 2162. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44709-1_26

2.Bogdanov, A., Khovratovich, D., Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. In: Lee, D.H., Wang, X. (eds) Advances in Cryptology – ASIACRYPT 2011. ASIACRYPT 2011. Lecture Notes in Computer Science, vol 7073. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25385-0_19

3. Increasing Usability of TLS Certificate Generation Process Using Secure Design; G. Iashvili, M. Iavich, A. Gagnidze, S. Gnatyuk; IVUS-2020; http://ceur-ws.org/Vol-2698/; 2020.

4.Canvel, B., Hiltgen, A., Vaudenay, S., Vuagnoux, M. (2003). Password Interception in an SSL/TLS Channel. In: Boneh, D. (eds) Advances in Cryptology - CRYPTO 2003. CRYPTO 2003. Lecture Notes in Computer Science, vol 2729. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45146-4_34

5. Brier, É.,Joye, M. (2002). Weierstraß Elliptic Curves and Side-Channel Attacks. In: Naccache, D., Paillier, P. (eds) Public Key Cryptography. PKC 2002. Lecture Notes in Computer Science, vol 2274.

Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45664-3_24

6. Goyal, V., O'Neill, A., Rao, V. (2011). Correlated-Input Secure Hash Functions. In: Ishai, Y. (eds) Theory of Cryptography. TCC 2011. Lecture Notes in Computer Science, vol 6597. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-19571-6_12

7. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Abstract book, EURO-ASIA FORUM IN POLITICS ECONOMICS AND BUSINESS – 2016, JULY 21-22, 2016, BELGRADE, SERBIA.