**Concepts of Cryptography**

*What is Cryptography?*

Cryptography, derived from its Greek origin “*Crypto.*” In its simplest form cryptography means secret, hidden or concealed writing.[1][6] The modern definition of encryption has expanded to the computerized encoding and decoding of information.[1][3] Cryptography is used whenever someone wants to send a secret message to someone else in a situation where an outside party could intercept and read that message.[3]

***Encoding*** *- The method of taking plaintext and converting it to unreadable or ciphertext.*

***Decoding*** *- The method of taking ciphertext and converting it to readable or plaintext.*

**Example**

* Passing a note to another student in class where a teacher or other student could intercept and read that note.
* Communication between your computer and *amazon.com* who is collecting your credit card information.

There are four goals of modern cryptography they include Confidentiality, Integrity, Authentication and Nonrepudiation. [3][4][8]

* **Confidentiality** – Information that is not publicly accessible without proof that the recipient is authorized to access it.
* **Integrity** – Proof that the data was not altered during transit by either malice or general interference. (hashing)
* **Authentication** - Validation that both clients connecting to one another are who they say they are.
* **Non-Repudiation** – A legal concept widely used in information security; non-repudiation is the assurance that someone cannot deny the validity, integrity, and authenticity of an encrypted digital message or signature. (hashing)

***CIA*** *- The first three can be remembered with the acronym CIA (Confidentiality, Integrity & Authentication).*

*Who uses Cryptography?*

In the past, cryptography was often used by generals to send orders to their armies. The most famous use of cryptography was during World War II where a cryptography machine called “Enigma” was developed and used by the German army to send secret messages throughout the war.[3][7] Modern uses for cryptography include keeping informational transactions between client and server (website transactions for example) private and secure.

*How Does Cryptography Work?*

Modern cryptography can be broken down into two main components, a cipher algorithm, and a key. A cipher algorithm is a mathematical formula designed to obscure the value and content of data.[4][8][10] A key is used to encrypt the data, and either that key or a complementary key is needed to decrypt the data back to its useful form.[4][8][10]

One of the best examples of early cryptography is the Caesar Cipher,[3][4][7] named after Julius Caesar. Here is an example of how the Caesar Cipher works.

**Example**

Take a piece of paper and write along the top edge the alphabet, then take another piece of paper and do the same thing. You should then have two lines of letters on separate pieces of paper that look like this:

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Now write your unencrypted message:   “*SEND MONEY TONIGHT*”

To ***key*** the cipher move one of your pieces of paper to the right one or more letters so that they no longer line up, that should look like this:

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
YZABCDEFGHIJKLMNOPQRSTUVWX

Now every time you see a letter of your message in the top line, write down instead the letter on the bottom line. Your unencrypted message “*SEND MONEY TONIGHT”* becomes:

*“QCLB KMLCW RMLGEFR”*

You have just performed a cryptographic transformation and encrypted your message.

*EXAMPLE TAKEN FROM INTRODUCTION TO ENCRYPTION AND CRYPTOGRAPHY*

All we must do now is ensure that the recipient of our message knows the encryption key (2) and the algorithm (Caesar Cipher).

As long the recipient knows the message was encrypted with the Caesar Cipher and that the encryption key is 2 they can put their lower line two places to the right, then by taking each letter of the message and writing down the letter immediately above it, they can re-create the original message.

*What is hashing and is it cryptography?*

A hash is a mathematical algorithm that converts an input of arbitrary length into an encrypted output of a fixed length. A hash is not cryptography; however, it is used in cryptography to provide ***integrity*** of data payloads transmitted over the Internet.[2][4][8]

*How does hashing work?*

A hashing algorithm creates a fixed length signature of a data payload by encoding it with a pre-shared key that only the sender and receiver know. Upon receipt of the data payload, the receiver then verifies the ***integrity*** of it by comparing signature by using the same hashing algorithm and key. The integrity of the data payload is valid when the signature from the hashing algorithm matches the content of the data payload. [4][8]

*Are hashes secure?*

Hashing algorithms are designed to be fast but not necessarily secure[2] methods do exist which can crack these hashes by using ***brute force*** and ***dictionary***, ***lookup table*** and ***rainbow table*** style attacks. These mechanisms to crack a hash are possible because each time a plaintext string is hashed, it generates the exact same hashed value.

***Brute Force Attack*** *– An attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by submitting many passwords or passphrases with the hope of eventually guessing correctly.*

***Dictionary Attack*** *– An attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possible combinations.*

***Lookup Table*** *– An extremely effective method for cracking many hashes of the same type very quickly.*

***Rainbow Table*** *– A password cracking method that uses a special table to crack password hashes in a database.*

**Example**

hash (“letmein”) = 0xf73bo1230k35n72nj523dtg9l4n2k6n24nv7i73gf36hf4ow9d4k4c2nm6m  
hash (“12345678”) = 4h5g2c9d0a34lk1k3n0sd8sdl4h54nm9g76dsj3n5ksb38j5ls93md0l3hz9d2  
hash (“baseball”) = 3n52k5kcn5kv9cma83ja83d430dm9c83m6n20cj67gb7ksnf8dgsmg056vm  
hash (“letmein”) = 0xf73bo1230k35n72nj523dtg9l4n2k6n24nv7i73gf36hf4ow9d4k4c2nm6m

To increase the security of password hashes an additional layer of security (randomness) needs to be added to the original plaintext value before hashing so that it will not generate the same hashed value each time. Randomizing these hashes by appending or prepending a random string, known as a ***salt***, can make it significantly more challenging for an attacker to use ***lookup tables*** or ***rainbow tables*** to crack these passwords by increasing the possible hashed values each password can have.[2]

***Salt*** *–**Random data that is used as additional input to a hashing algorithm, password or passphrase. This randomness is used to safeguard passwords in storage.*

**Example**

hash (“letmein” + “F34564R8”) = 8f3k9j3hdk98jk30lsvn9al30lfb48slhbtwe9uka903bwj380dsfj3v2nf930nk3  
hash (“letmein” + “Y456f3q9”) = ber5jg0qhekgl8dkjhl52309uwlkmcbkuw385b9smqnv9c234calq95nf34flql  
hash (“letmein” + “56hwF3h8”) = w2lkg034fmwprm80n59fdmal40djwbel46n32ldn2la9702nd772ha95lg06j

*Encryption In Everyday Life*

PKI

WHO USES IT

WHAT IS IT USED FOR

WHERE IS IT USED

WHEN IS IT USED

WHY IS IT USED

HOW IS IT USED

ENCRYPTION AT REST

ENCRYPTION IN TRANSIT

**REFERENCES**

1. Merriam-Webster. (n.d.). *Cryptography*. Retrieved November 4, 2021, from https://www.merriam-webster.com/dictionary/cryptography
2. McAfee. (2016). *What is a Salt and How Does It Make Password Hashing More Secure*. Retrieved November 4, 2021, from https://www.mcafee.com/blogs/enterprise/cloud-security/what-is-a-salt-and-how-does-it-make-password-hashing-more-secure/
3. ArticSoft. (n.d.). *Introduction to Encryption & Cryptography*. Retrieved November 4, 2021, from https://www.articsoftpgp.com/encryption.htm
4. Fraser, D. (2018). *What are encryption keys and how do they work*. November 4, 2021, from https://medium.com/codeclan/what-are-encryption-keys-and-how-do-they-work-cc48c3053bd6
5. Smith. B. (2018). *Prime numbers keep your encrypted messages safe — here's how*. Retrieved November 4, 2021, from https://www.abc.net.au/news/science/2018-01-20/how-prime-numbers-rsa-encryption-works/9338876
6. WordNik. (n.d.). *Crypto*. November 4, 2021, from https://www.wordnik.com/words/crypto
7. Moore, K. et.al. (n.d.). *Enigma Machine.* November 4, 2021, from https://brilliant.org/wiki/enigma-machine
8. Beaming. (n.d.). *What is cryptography and how do we use it in modern day computing*. November 4, 2021, from https://www.beaming.co.uk/knowledge-base/techs-cryptography-use-modern-day-networking/
9. Cryptomathic. (n.d.). *What is non-repudiation*. November 4, 2021, from https://www.cryptomathic.com/products/authentication-signing/digital-signatures-faqs/what-is-non-repudiation
10. IBM. (n.d.). Cipher algorithms and keys. November 4, 2021, from https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-cipher-algorithms-keys