

Cryptography

What are Encryption Keys

Symmetric vs Asymmetric

Sam Stoner IUS 2020 Student Conference

John Doyle Sponsor

Objective

- ▶ The goal of my research was to better understand what encryption keys are, symmetric vs asymmetric encryption, and mainly to learn/implement some of the more common algorithms used for encryption



Encryption Keys

Used to help encrypt and decrypt information

Created and used in conjunction with these encryption algorithms(mentioned later in slides) in order to keep data secure

The goal is to go from Plaintext -> Ciphertext or vice versa while keeping the information as safe as possible

Symmetric Encryption



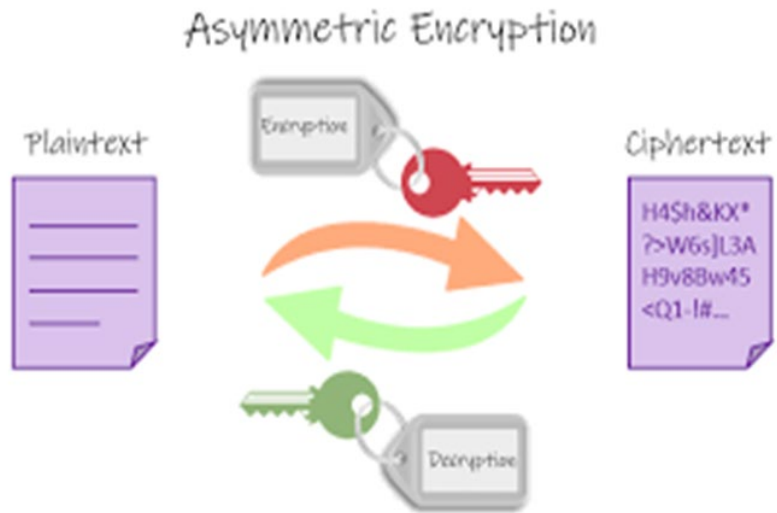
- ▶ Type of encryption that is executed with only one secret key
- ▶ This (singular)key which is sent before sending the messages, is then used to both encode and decode the information
- ▶ Is preferred over asymmetric when large sets of data are being used as it can be processed much faster...(less CPU cycles)

AES Encryption

- ▶ 128, 192, or 256-bit keys
- ▶ If a 128-bit key were used, a brute force attack would have to go through 2^{128} potential values or $3.40e+38$
- ▶ An important part of this encryption is the idea of key expansion. This involves taking the initial key given and then using it to create this series of more keys.
- ▶ Depending on the bit key size, this type of encryption will go through multiple rounds of keys to further encrypt your message(9,11,13) many times.
- ▶ Each time, these bytes will be replaced/substituted further encrypting the message
- ▶ Since it's symmetric the key is secret!

```
run:  
Plaintext Value: IUS-StudentConfecerence-2020-Sam_Stoner  
Encrypted String: 0mXGWCvZVHIFKvtaICcp12KJZ7F/UihlpqTD8KtAKp1IKrNCE2u8/53juN+4qKNO  
Decrypted/Original Value: IUS-StudentConfecerence-2020-Sam_Stoner  
BUILD SUCCESSFUL (total time: 0 seconds)
```

Asymmetric Encryption



- ▶ Type of encryption that is executed using two different keys, one being the public and the other being the private key
- ▶ Generally this public key is used to encrypt the message, while the private key which is sent only to the desired recipient, is used to decrypt the encrypted message that is sent
- ▶ The flow generally follows like so plaintext -> encryption algorithm -> public and private keys -> ciphertext -> decryption. In other words, the main difference is the added public key when compared to symmetric encryption.

RSA Encryption Algorithm



Uses prime factorization algorithm generally in a $n = p * q$ format which is currently beyond computing capabilities on a normal system



You then find the modulus and finally Euler's totient function is used with the prime factors to get/calculate keys.



Slower algorithm and because of such, usually isn't used to encrypt user data



Because of this, what I learned during this study is a lot of times the information is encrypted with a symmetric key and then that key will be encrypted further with this RSA asymmetric algorithm



This works as only a select amount of individuals will then have this RSA private key

ECC Encryption

ECC is a type of public key encryption based on an actual elliptic curve theory that can be used to create these smaller keys

With these smaller keys generally comes faster speeds and just overall better efficiency

ECC also is said to use less computing power and battery resource usage making it a strong contender for the future world of cryptography especially within mobile devices

Takeaways

- ▶ During my research, I learned that there are many encryption algorithms, both symmetric and asymmetric, that are used to this day to keep our information secured.
- ▶ Used in conjunction often as symmetric keys have a faster encryption speed while asymmetric keys help with the key distribution process and just further the safety of the information being sent.
- ▶ Many of these algorithms that are commonly used have been around for years and are most likely going to be used for quite some time as they work well and are hard for most modern computers to crack to this day.
- ▶ Will be interesting to see if any new big algorithms will take the throne, but currently I'd say were in good hands.

References

- ▶ Stallings, W., & Brown, L. (2019). *Computer security: principles and practice*. Harlow, United Kingdom: Pearson.
- ▶ By. (2020, March 3). Symmetric vs. Asymmetric Encryption. Retrieved from <https://www.101computing.net/symmetric-vs-asymmetric-encryption/>