# Asymmetric Versus Symmetric Algorithms

Tyler Chotikamars

CYB 400 Cryptography

Michael Hayden

January 10th, 2022

Cryptographic algorithms for encrypting and decrypting data include symmetric cryptographic algorithms as well as asymmetric cryptographic information. There are many reasons as to why people might need to encrypt and decrypt information, one notable reason includes transporting sensitive data. In this case, ensuring that the CIA triad of confidentiality, integrity, and availability is crucial to making sure that the data is safe and untampered with. Within this asymmetric versus symmetric algorithms paper, we'll be taking a look at the difference between both encryption methods and comparing different types of encryptions within each category, as well as explaining the differences in encryption key sizes for both methods.

Symmetric cryptographic algorithms use the same single key to encrypt and decrypt a document. This method is designed to be used for encryption as well as decryption. The only way an attacker could decrypt an encrypted message would be to obtain the key for the encrypted documents. This means that it is very important to keep the key private, symmetric cryptographic algorithms can also be referred to as private key cryptography for this reason (Ciampa, 2018). Some common methods of encryption that fit the requirements of symmetric cryptography include the Data Encryption Standard, Triple Data Encryption Standard, Advanced encryption Standard, and Blowfish.

Asymmetric cryptography uses public key cryptography where there are two keys instead of one. There is a private key and a public key which are mathematically related where the public key can be freely distributed to everyone. The private key in this case is known to only the individual who owns it. Some key aspects of asymmetric cryptography include key pairs where there are two keys required, public and private key, and both directions where keys work in both directions. Here a document can be encrypted with a public key and be decrypted with a corresponding private key as well as having a document encrypted with a private key and

decrypted with its public key (Ciampa, 2018). Common asymmetric cryptographic algorithms include Elliptic Curve Cryptography, RSA, Digital Signature Algorithm, and Key exchange including DH.

Symmetric cryptography algorithms such as Data Encryption Standard (DES) makes use of 56 bits and has been officially adopted by the U.S. government as the standard for encrypting non-classified information. Triple Data Encryption Standard (3DES) was developed to replace AES. This method uses three rounds of encryption instead of one to encrypt information. Here, 48 iterations of encryption are used (3 x 16) and is better for hardware than it is for software. Advanced Encryption Standard (AES) is a symmetric cipher and is approved by the NIST. Here AES uses three steps on blocks of 128 bits of plaintext. Here depending on the key size a different amount rounds are used, where in each round the bytes are rearranged using special multiplication. There have been no successful attacks against AES. The last symmetric cryptographic algorithm to be covered is Blowfish. Blowfish operates on 64-bit blocks and can have a key length ranging from 32 to 448 bits. Blowfish was created to run on 32-bit computers with no significant weakness detected. There is another version called Twofish which is stronger but not as widely used (Ciampa, 2018).

Asymmetric encryption methods work different and therefore have different methods of encryption. These can include methods such as key exchange. Diffie-Hellman (DH) is a type of key exchange that enables both users to agree upon a large prime number and a related integer. Both numbers can be made public however they must use mathematical computations and exchanges to separately create the same key. Another asymmetric algorithm includes RSA which was published in 1977 and is named after its three developers. Here, RSA multiplies two large prime numbers and multiplied together to create *n.* Then variable m is

created by performing p-1 * q-1. Here *e* is found and ensured that it and *m* have no common divisor other than 1. Then variable *d* is found with the equation *d = (1 = n*m)/e.* Elliptic Curve Cryptography (ECC) uses an elliptic curve cryptography rather than using large prime numbers. Within this method two points on a graph are shared by users while one user chooses a secret random number. The other use does the same and they exchange messages based on the public keys that can be generated by a private key on the elliptic curve. Digital Signature Algorithm (DSA) is used to provide proofs. This algorithm ensures that attackers cannot pretend to be someone who they are not by allowing them to encrypt messages with a public key and send it out. Digital signatures are used here to verify who the sender is. DSA is used by the U.S. federal government for digital signatures and is the standard provided by the NIST. Digital signatures work both ways and can be verified by using a public key to decrypt the digital signature.

There are different use cases for both types of algorithms (symmetric and asymmetric). Symmetric key sizes are usually smaller therefore can be encrypted and decrypted faster. This is because symmetric algorithms use one key for both encryption and decryption while asymmetric encryption makes used of the public key for encryption and private key for decryption. Asymmetric algorithms usually also have larger bit sizes making it longer for them to encrypt and decrypt information. Encryption is crucial to everyone using the internet as it provides a means to keep data secure while it is in transport, as well as it protects databases.

References:

Ciampa, M. (2018). *CompTIA security+ guide to network security fundamentals* (6th ed.). Cengage Learning.