Name: Date: Class:

Cryptography Background Reading

Note: The following is based on this article from IBM: https://www.ibm.com/think/topics/cryptography.

What is cryptography?

Cryptography is the practice of developing and using coded algorithms to protect and obscure transmitted information so that it may only be read by those with the permission and ability to decrypt it. Put differently, cryptography obscures communications so that unauthorized parties are unable to access them.
In our modern digital age, cryptography has become an essential cybersecurity tool for protecting sensitive information from hackers and other cybercriminals.

Derived from the Greek word “kryptos,” meaning hidden, cryptography translates to “hidden writing.” It can be used to obscure any form of digital communication, including text, images, video, or audio. In practice, cryptography is mainly used to transform messages into an unreadable format (known as ciphertext) that can only be decrypted into a readable format (known as plain text) by the authorized intended recipient by using a specific secret key.

Cryptology, which encompasses both cryptography and cryptanalysis, is deeply rooted in computer science and advanced mathematics. The history of cryptography dates to ancient times when Julius Caesar created the Caesar cipher to obscure the content of his messages from the messengers who carried them in the first century B.C.. Today, organizations like the National Institute of Standards and Technology (NIST) continue to develop cryptographic standards for data security.

Core tenets of modern cryptography

Modern cryptography has grown significantly more advanced over time. However, the general idea remains the same and has coalesced around four main principles.

- Confidentiality: Encrypted information can only be accessed by the person for whom it is intended and no one else.
- Integrity: Encrypted information cannot be modified in storage or in transit between the sender and the intended receiver without any alterations being detected.
- Non-repudiation: The creator or sender of encrypted information cannot deny their intention to send the information.
- Authentication: The identities of the sender and receiver, as well as the origin and destination of the information are confirmed.

Why cryptography is important

In today’s digital landscape, cryptography plays a vital role in our daily lives, ensuring that sensitive data like credit card numbers, e-commerce transactions and even WhatsApp messages remain confidential and secure.

On a macro level, advanced cryptography is crucial for maintaining national security, safeguarding classified information from potential threat actors and adversaries.

Name: Date: Class:

Common uses for cryptography
These are some of the most common cases for cryptography.

Passwords
Cryptography is frequently used to validate password authenticity while also obscuring stored passwords. In this way, services can authenticate passwords without the need to keep a plain text database of all passwords which might be vulnerable to hackers.

Cryptocurrency
Cryptocurrencies like Bitcoin and Ethereum are built on complex data encryptions that require significant amounts of computational power to decrypt. Through these decryption processes, new coins are "minted" and enter circulation. Cryptocurrencies also rely on advanced cryptography to safeguard crypto wallets, verify transactions, and prevent fraud.

Secure web browsing
When browsing secure websites, cryptography protects users from eavesdropping and man-in-the-middle (MitM) attacks. The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols rely on public key cryptography to protect data sent between the web server and client and establish secure communications channels.

Electronic signatures
Electronic signatures, or e-signatures, are used to sign important documents online and are frequently enforceable by law. Electronic signatures created with cryptography can be validated to prevent fraud and forgeries.

Authentication
In situations where identity authentication is necessary, such as logging in to an online bank account or accessing a secure network, cryptography can help confirm or verify a user's identity and authenticate their access privileges.

Secure communications
Whether sharing classified state secrets or simply having a private conversation, end-to-end encryption is used for message authentication and to protect two-way communications like video conversations, instant messages, and email. End-to-end encryption provides a high level of security and privacy for users and is widely used in communication apps like WhatsApp and Signal.

Types of cryptography
There are two main types of encryption in use today: symmetric cryptography and asymmetric cryptography. Both types use keys to encrypt and decrypt data sent and received. There are also hybrid cryptosystems that combine both.

Name: Date: Class:

A cryptosystem is considered symmetrical when each party—sender and receiver—uses the same key to encrypt and decrypt data. Algorithms such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are symmetric systems.

Asymmetric cryptography uses multiple keys—some shared and some private. In this way, the sender and receiver of an encrypted message have asymmetrical keys, and the system is asymmetrical. RSA—named after its progenitors Rivest, Shamir and Adleman—is one of the most common public key encryption algorithms.

While asymmetric systems are often considered to be more secure due to their use of private keys, the true measure of a system's strength is more dependent on key length and complexity.

Symmetric cryptography

Symmetric cryptography uses a shared single key for both encryption and decryption. In symmetric cryptography, both the sender and receiver of an encrypted message will have access to the same secret key.

Caesar's cipher is an early example of a single key system. This primitive cipher worked by transposing each letter of a message forward by three letters, which would turn the word "cat" into "fdw" (although Caesar would have probably used the Latin word "cattus"). Since Caesar's generals knew the key, they would be able to unscramble the message by simply reversing the transposition. In this way, symmetrical cryptosystems require each party to have access to the secret key before the encrypting, sending, and decrypting of any information.

Some of the main attributes of symmetric encryption include:

- Speed: The encryption process is comparatively fast.
- Efficiency: Single key encryption is well suited for large amounts of data and requires fewer resources.
- Confidential: Symmetrical encryption effectively secures data and prevents anyone without the key from decrypting the information.

Asymmetric cryptography

Asymmetric cryptography (also referred to as public-key cryptography) uses one private key and one public key. Data that is encrypted with a public and private key requires both the public key and the recipient's private key to be decrypted.

Public-key cryptography enables secure key exchange over an insecure medium without the need to share a secret decryption key because the public key is only used in the encryption, but not the decryption process. In this way, asymmetric encryption adds an additional layer of security because an individual's private key is never shared.

Some of the main attributes of symmetric encryption include:

- Security: Asymmetric encryption is considered more secure.
- Robust: Public-key cryptography offers more benefits, providing confidentiality, authenticity, and non-repudiation.
- Resource intensive: Unlike single key encryption, asymmetrical encryption is slow and requires greater resources, which can be prohibitively expensive in some cases.

Cryptographic keys and key management

Cryptographic keys are essential for the secure use of encryption algorithms. Key management is a complex aspect of cryptography involving the generation, exchange, storage, use, destruction, and replacement of keys. The Diffie-Hellman key exchange algorithm is a method used to securely exchange cryptographic keys over a public channel. Asymmetric key cryptography is a critical component in key exchange protocols.

Unlike Caesar's cipher, which used a shifted Roman alphabet as a key, modern keys are far more complex and typically contain 128, 256 or 2,048 bits of information. Advanced cryptographic algorithms use these bits to rearrange and scramble the plain text data into ciphertext. As the number of bits increases, the number of total possible arrangements of the data rises exponentially.

Caesar's cipher uses few bits, and it would be easy for a computer to decrypt (even without the secret key) by simply trying all the possible arrangements of the scrambled ciphertext until the entire message was transformed into readable plain text. Hackers call this technic a brute-force attack.

Adding more bits makes brute-force attacks prohibitively difficult to compute. While a 56-bit system can be brute forced in 399 seconds by today's most powerful computers, a 128-bit key would require 1.872 x 1037 years. A 256-bit system would take 3.31 x 1056 years.

For reference, the entire universe is believed to have existed for only 13.7 billion years, which is less than a percent of the time it would take to brute force either a 128-bit or 256-bit cryptosystem.

Cryptographic algorithms and encryption methods

An encryption algorithm is a component of a cryptosystem that performs the transformation of data into ciphertext. Block ciphers such as AES operate on fixed-size blocks of data by using a symmetric key for encryption and decryption. Stream ciphers, conversely, encrypt data one bit at a time.

Digital signatures and hash functions

Digital signatures and hash functions are used for authentication and ensuring data integrity. A digital signature created with cryptography provides a means of non-repudiation, ensuring that a message's sender cannot deny the authenticity of their signature on a document.

Hash functions, such as the Secure Hash Algorithm 1 (SHA-1), can transform an input into a string of characters of a fixed length, which is unique to the original data. This hash value helps in verifying the

integrity of data by making it computationally infeasible to find two different inputs that might produce the same output hash.

The future of cryptography
In keeping pace with advancing technology and increasingly sophisticated cyberattacks, the field of cryptography continues to evolve. Next-generation advanced protocols such as quantum cryptography and elliptic curve cryptography (ECC) represent the cutting edge of cryptographic techniques.

Elliptical curve cryptography
Considered to be one of the main focal points of the next generation, elliptic curve cryptography (ECC) is a public-key encryption technique based on elliptic curve theory that can create faster, smaller, and more efficient cryptographic keys.

Traditional asymmetric cryptosystems, while secure, are difficult to scale. They require a lot of resources and become sluggish as they are applied to larger amounts of data. Further, attempts to improve the security of public key cryptosystems to evade increasingly powerful attacks require increasing the bit length of the public and private keys, which significantly slows the encryption and decryption process.

First-generation public-key cryptosystems are built on the mathematic functions of multiplication and factoring, in which public and private keys reveal the specific mathematical functions necessary to both encrypt plain text and decrypt ciphertext. These keys are made by multiplying prime numbers. ECC uses elliptical curves—equations that can be represented as curved lines on a graph—to generate public and private keys based on different points on the line graph.

In a world where we are increasingly reliant on devices with less computing power, such as mobile phones, ECC provides an elegant solution based on the obscure mathematics of elliptical curves to generate smaller keys that are more difficult to crack.

The advantages of ECC over previous public-key cryptosystems are undisputed, and the U.S. government, Bitcoin, and Apple's iMessage service already use it. While first-generation systems such as RSA are still effective for most settings, ECC is poised to become the new standard for privacy and security online—especially as the tremendous potential of quantum computing looms over the horizon.

Though quantum computers are still in their infancy and difficult to build, program and maintain, the potential increase in computation power would render all known public-key encryption systems insecure, since a quantum machine could theoretically achieve a brute-force attack significantly faster than classical computers.

Quantum cryptography
Quantum cryptography uses the principles of quantum mechanics to secure data in a way that is immune to many of the vulnerabilities of traditional cryptosystems. Unlike other types of encryption that rely on mathematic principles, quantum cryptography is based on physics to secure data in a way that is

theoretically immune to hackers. Because it is impossible for a quantum state to be observed without it being changed, any attempts to covertly access quantum encoded data would be immediately identified. Originally theorized in 1984, quantum encryption functions by using photon light particles sent across a fiberoptic cable to share a private key between the sender and receiver. This stream of photons travel in a single direction and each one represents a single bit of data, either 0 or 1. A polarized filter on the sender's side changes the physical orientation of each photon to a specific position, and the receiver uses two available beam splitters to read the position of each photon. The sender and receiver compare the sent photon positions to the decoded positions, and the set that matches is the key.

Quantum cryptography provides many benefits over traditional cryptography because it does not rely on potentially solvable math equations to secure encrypted data. It also prevents eavesdropping, since quantum data cannot be read without also being changed, and quantum cryptography can also integrate well with other types of encryption protocols. This type of cryptography enables users to digitally share a private encryption key that cannot be copied during transit. Once this key is shared, it can be used to encrypt and decrypt further messages in a way that has almost no risk of being compromised.

However, quantum cryptography also faces many challenges and limitations that have yet to be solved and currently prevents practical use of quantum cryptography. As quantum computing has yet to cross over from proofs of concept into practical application, quantum cryptography remains prone to error due to unintended changes in photon polarization.

Quantum cryptography also requires specific infrastructure. Fiber optic lines are necessary for transferring photons and have a limited range of typically about 248 to 310 miles, which computer science researchers are working to extend. Additionally, quantum cryptography systems are limited by the number of destinations where they can send data. Since these types of systems rely on the specific orientation of unique photons, they are incapable of sending a signal to more than one intended recipient at any time.