**TEAM 1:**

SHIVA A

MRINALINI R S

DIKSHITHA V N

GM AMARNATH

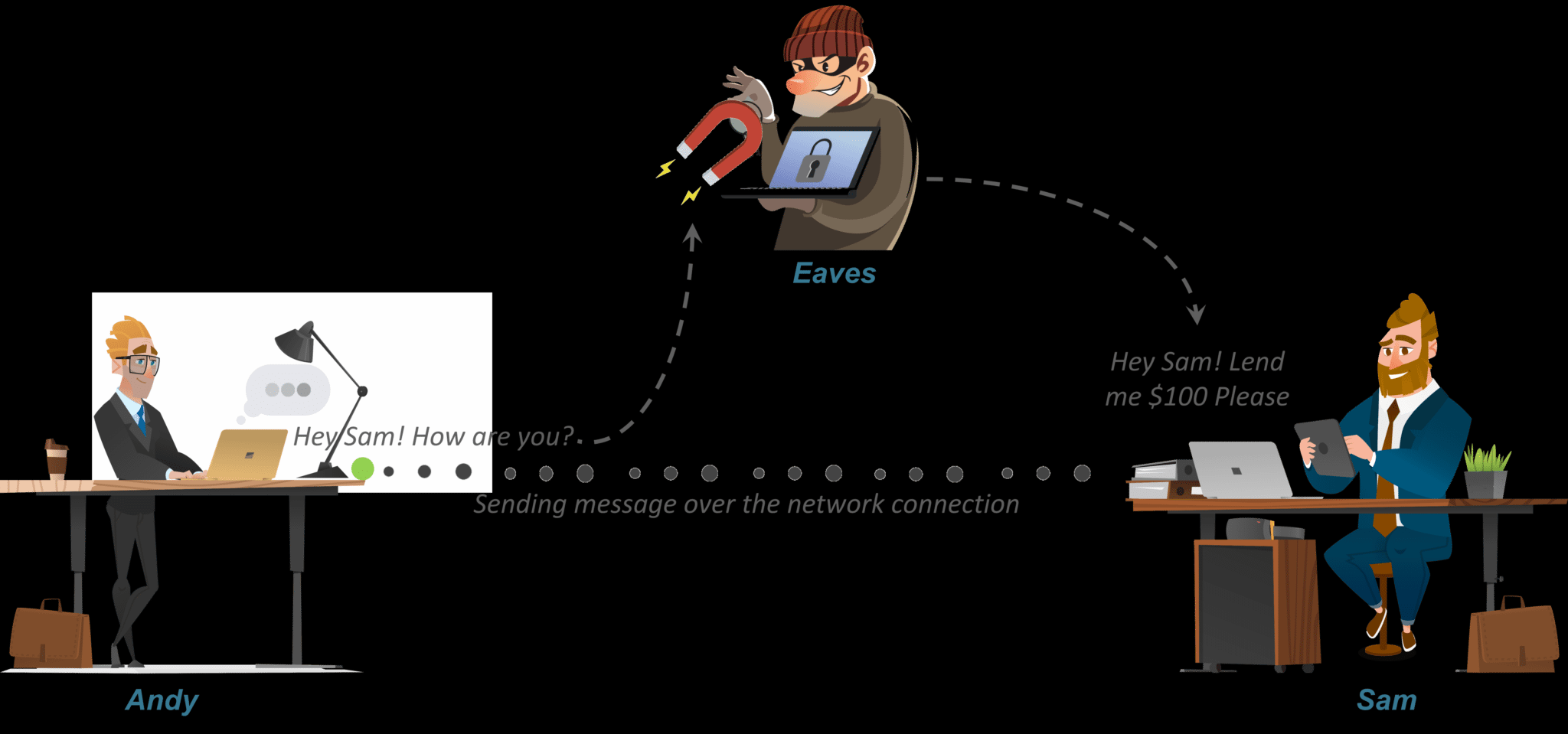
**Table of contents:**

1. Description of Cryptography
2. Terminology of Cryptography
3. History of Cryptography
4. Techniques used for Cryptography
5. Features of Cryptography
6. Types of Cryptography
7. Working algorithm of Cryptography
8. Applications and Conclusion

***CRYPTOGRAPHY:***

CRYPTOGRAPHY is the practice and study of techniques for secure communications in the presence of third parties called, “adversaries”.

The word, “CRYPTOGRAPHY” is derived from two words, ‘Kryptos’-which means,”hidden/secret”, and “graphein”-which means, “to write”.



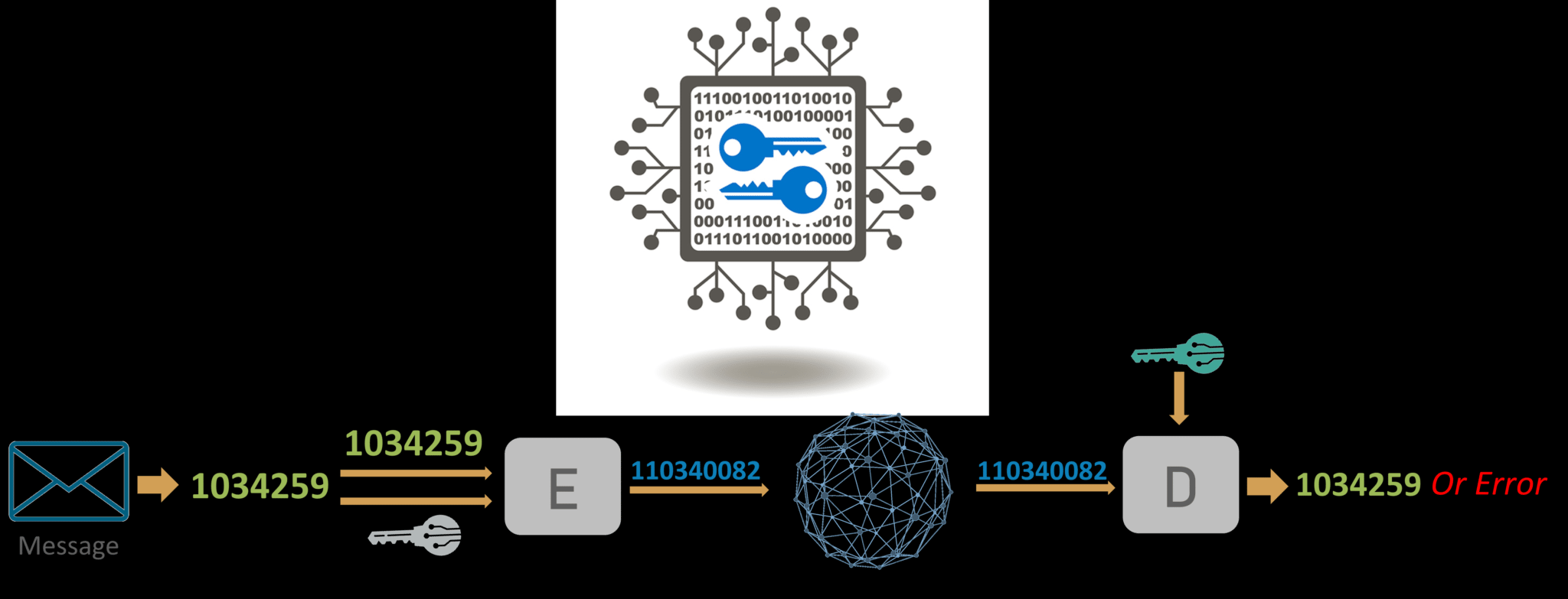
More generally, cryptography is about constructing and analysing the protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication and non repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, and communication science. Applications of cryptography include electronic

commerce, chip based payment cards, digital currencies, computer passwords, and military communications.

Cryptography prior to the modern age was effectively synonymous with *encryption,* the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to

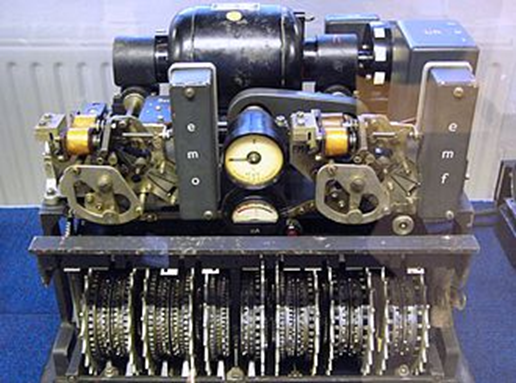
preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary.  Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorisation algorithms, and faster computing technology require these solutions to be continually adapted. There exist information theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to use in practice than the best theoretically breakable but computationally secure mechanisms.



The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit

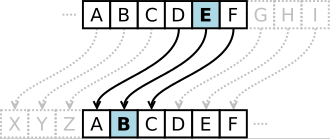
investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.



The above picture shows the German Lorenz Cipher machine, used in World War II, to encrypt very high-level staff messages.

TERMINOLOGY:

The first use of the term, “cryptograph” dates back to the 19th century, originated from “The Gold-Bug”, a novel by Edgar Allan Poe.



The above picture depicts that the alphabet shift ciphers are believed to have been used by Julius Caeser over 2000 years ago. This is an example with k=3. [The letters in an alphabet are shifted 3 in one direction to encrypt and three in other direction to decrypt]

HISTORY:

Before the modern era, cryptography focused on message encryption. Encryption attempted to ensure secrecy in communications, such as those of spies, military leaders and diplomats. In recent decades, the field has expanded beyond confidentiality concerns

to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure competition among others.

TECHNIQUES USED FOR CRYPTOGRAPHY:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

FEATURES OF CRYPTOGRAPHY:

**Confidentiality:**  
Information can only be accessed by the person for whom it is intended and no other person except him can access it.

**Integrity:**  
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

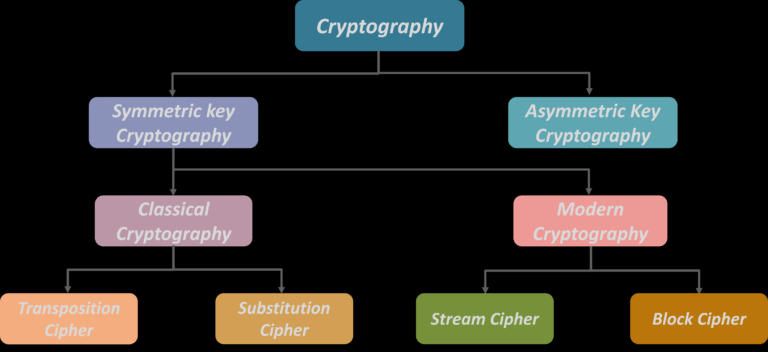
**Non-repudiation:**  
The creator/sender of information cannot deny his or her intention to send information at later stage.

**Authentication:**  
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

TYPES OF CRYPTOGRAPHY:

There are three types of cryptography in general.

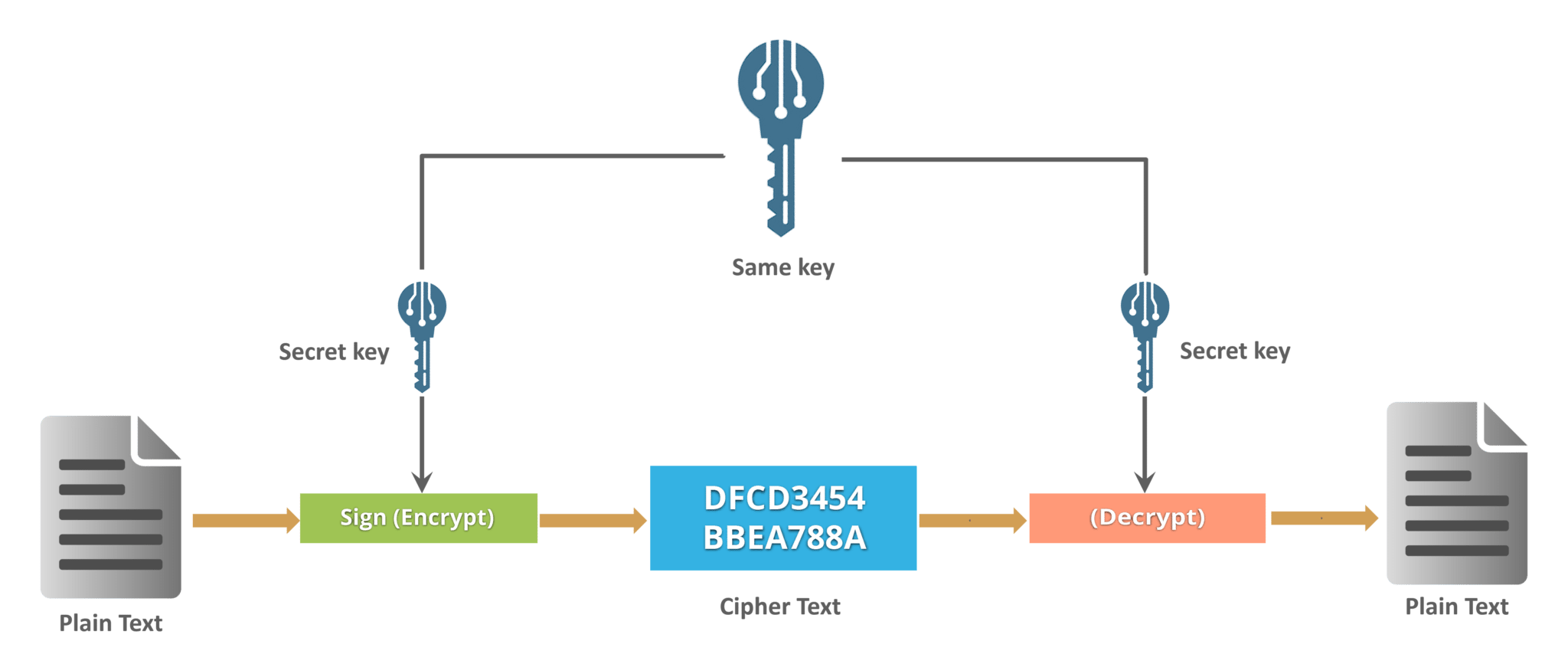
1. **Symmetric Key Cryptography:**  
   It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
2. **Hash Functions:**  
   There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:**  
   Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.



HOW DOES VARIOUS CRYPTOGRAPHIC ALGORITHMS WORK?

**Symmetric Key Cryptography**

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The most popular symmetric–key system is the Data Encryption Standard (DES)

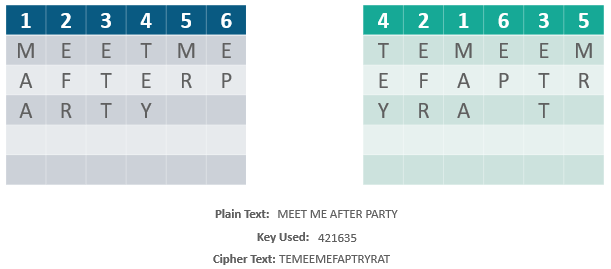


**Transposition Ciphers**

In Cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.

That is, the order of the units is changed (the plaintext is reordered). Mathematically, a bijective function is used on the characters’ positions to encrypt and an inverse function to decrypt.

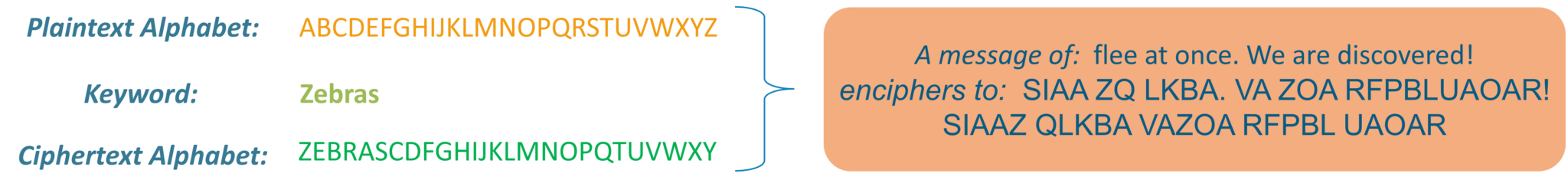
***Example:***

******

 Method of encryption by which units of plaintext are replaced with ciphertext, according to a fixed system; the “units” may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.

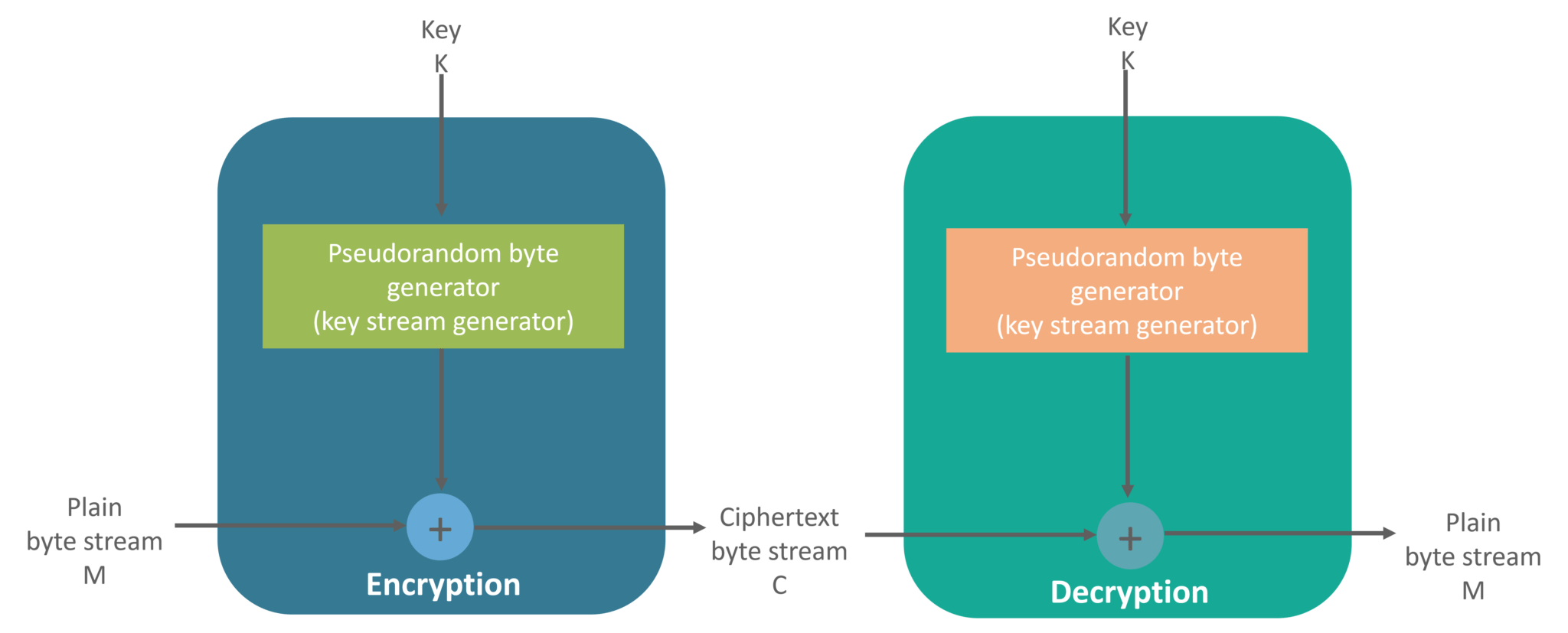
***Example:***

Consider this example shown on the slide: Using the system just discussed, the keyword “zebras” gives us the following alphabets:



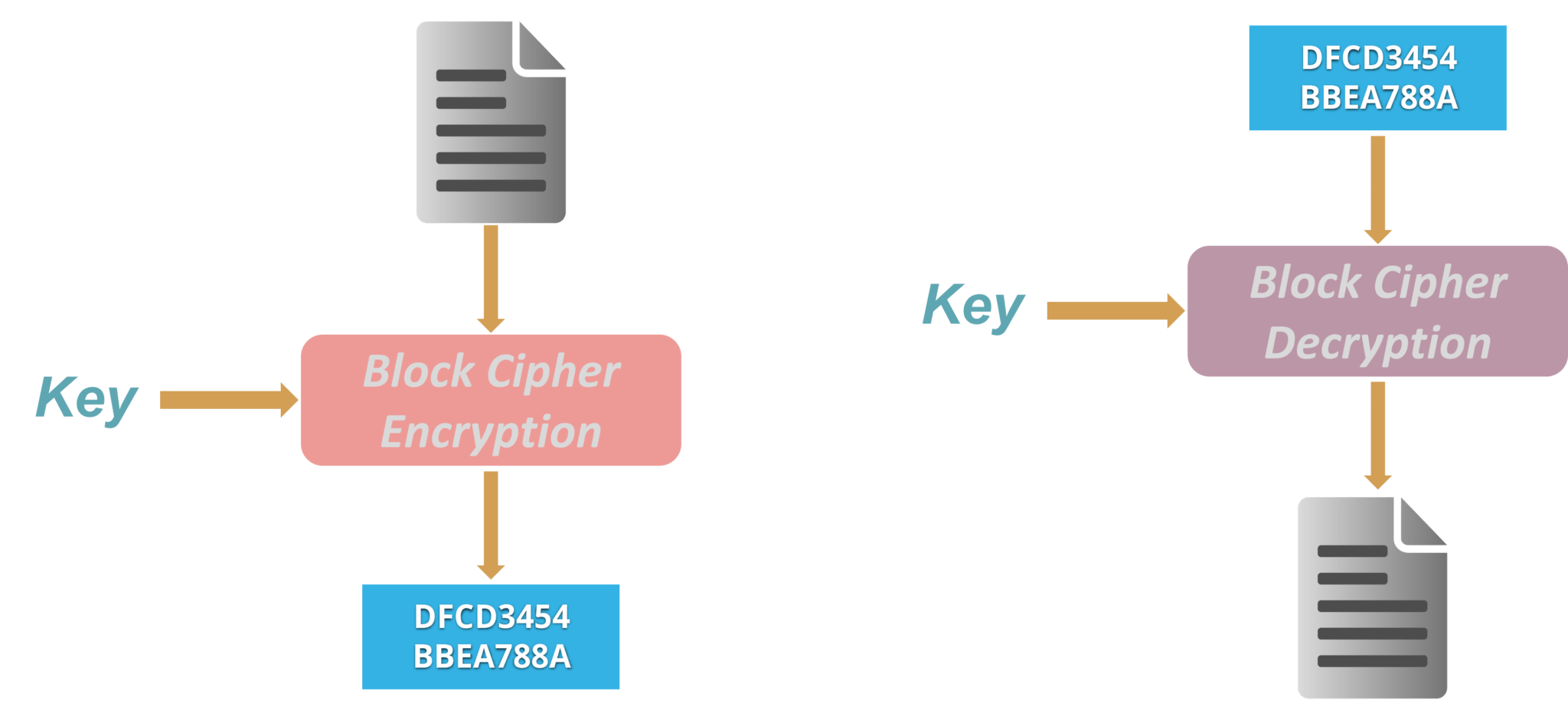
### ****Stream Cipher****

*Symmetric or secret-key encryption algorithm that encrypts a single bit at a time. With a Stream Cipher, the same plaintext bit or byte will encrypt to a different bit or byte every time it is encrypted.*

**

### ****Block Cipher****

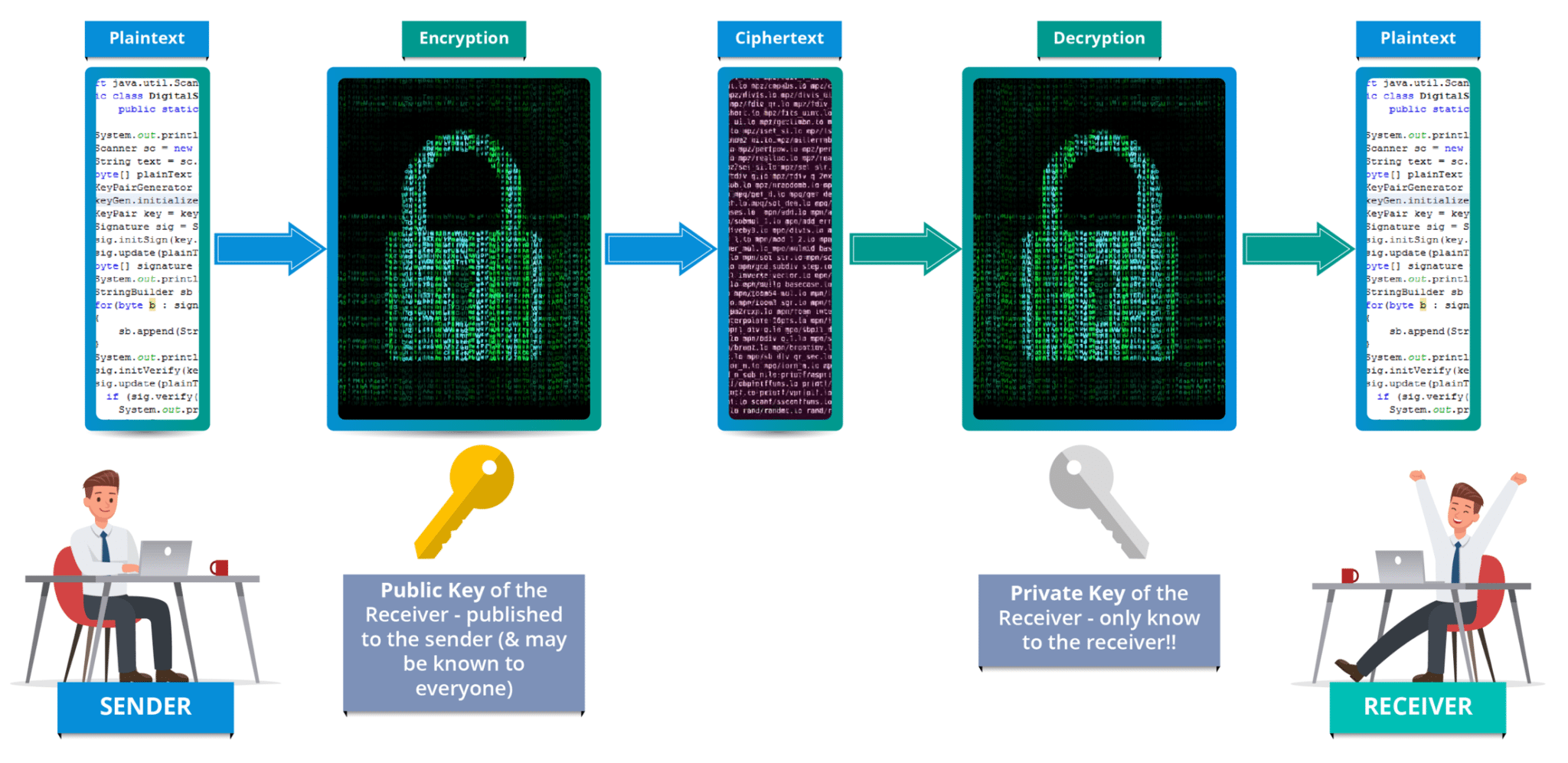
 An encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers



**Example:**A common block cipher, AES, encrypts 128-bit blocks with a key of predetermined length: 128, 192, or 256 bits. Block ciphers are pseudorandom permutation (PRP) families that operate on the fixed size block of bits. PRPs are functions that cannot be differentiated from completely random permutations and thus, are considered reliable until proven unreliable.

### ****Asymmetric Key Encryption (or Public Key Cryptography)****

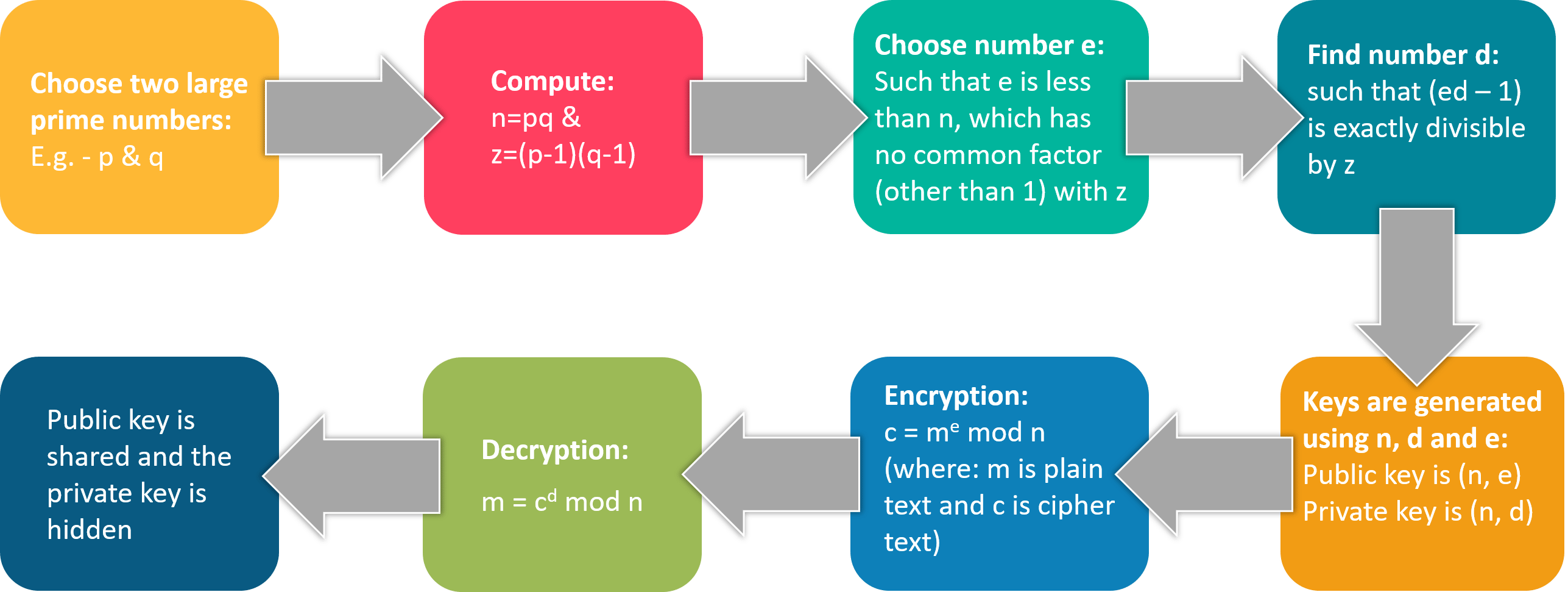
The encryption process where different keys are used for encrypting and decrypting the information. Keys are different but are mathematically related, such that retrieving the plain text by decrypting ciphertext is feasible.



RSA is the most widely used form of public key encryption,

### ****RSA Algorithm****

* RSA stands for Rivest, Shamir, and Adelman, inventors of this technique
* Both public and private key are interchangeable
* Variable Key Size (512, 1024, or 2048 bits)

Here’s how keys are generated in RSA algorithm**

[[](https://www.edureka.co/cybersecurity-certification-training)](https://www.edureka.co/cybersecurity-certification-training" \t "_blank)

APPLICATIONS AND CONCLUSION:

Cryptography plays a crucial role in encrypting modern day applications such as WhatsApp, Digital Signatures and HTTPS. Cryptography will continue to play a very vital and crucia role in securing all aspects of our technical world.