Symmetric Encryption

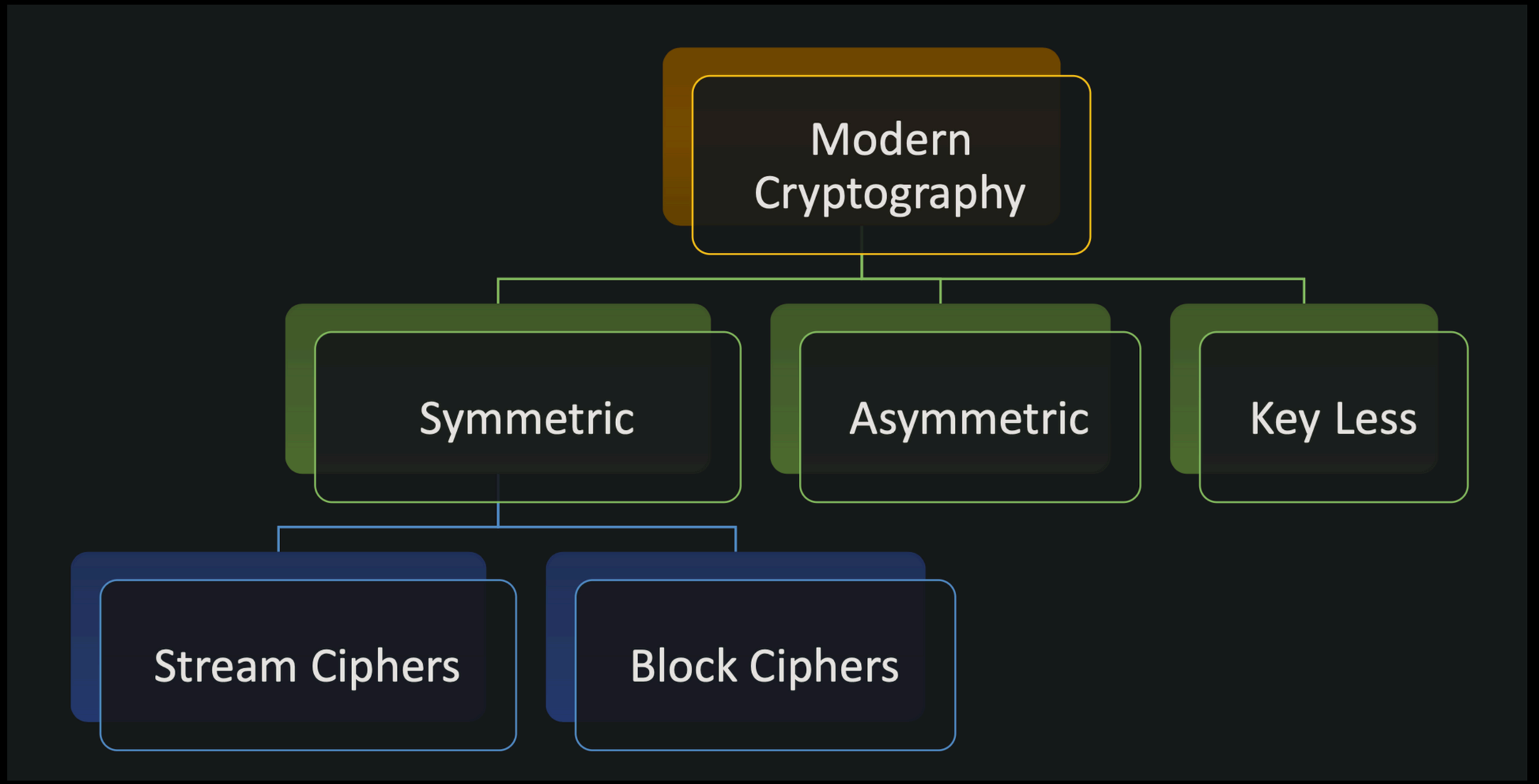
“The art of secrets shared… but not exposed.”

CЯ4CK1NG-THΞ-C0D3

Today’s Roadmap

- The Core Idea – Symmetry in Encryption
- Block vs Stream Ciphers
- The DES, 3DES and AES Standards

Before we get into it, lets classify modern cryptology-

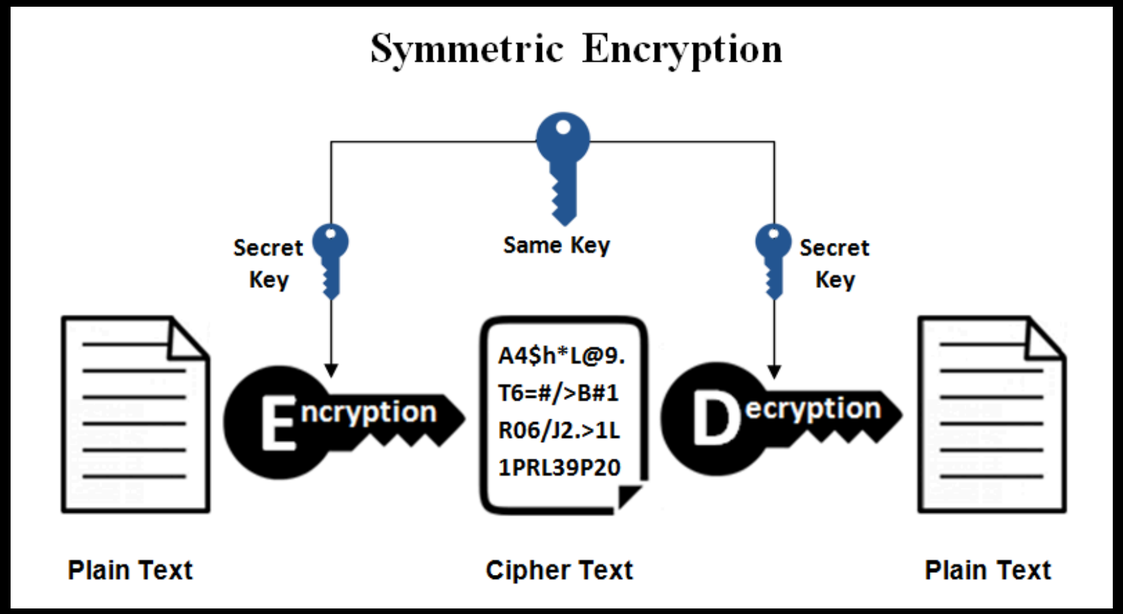

Modern Cryptography
Symmetric
Asymmetric
Key Less
Stream Ciphers
Block Ciphers

So let's get into the crux of it.

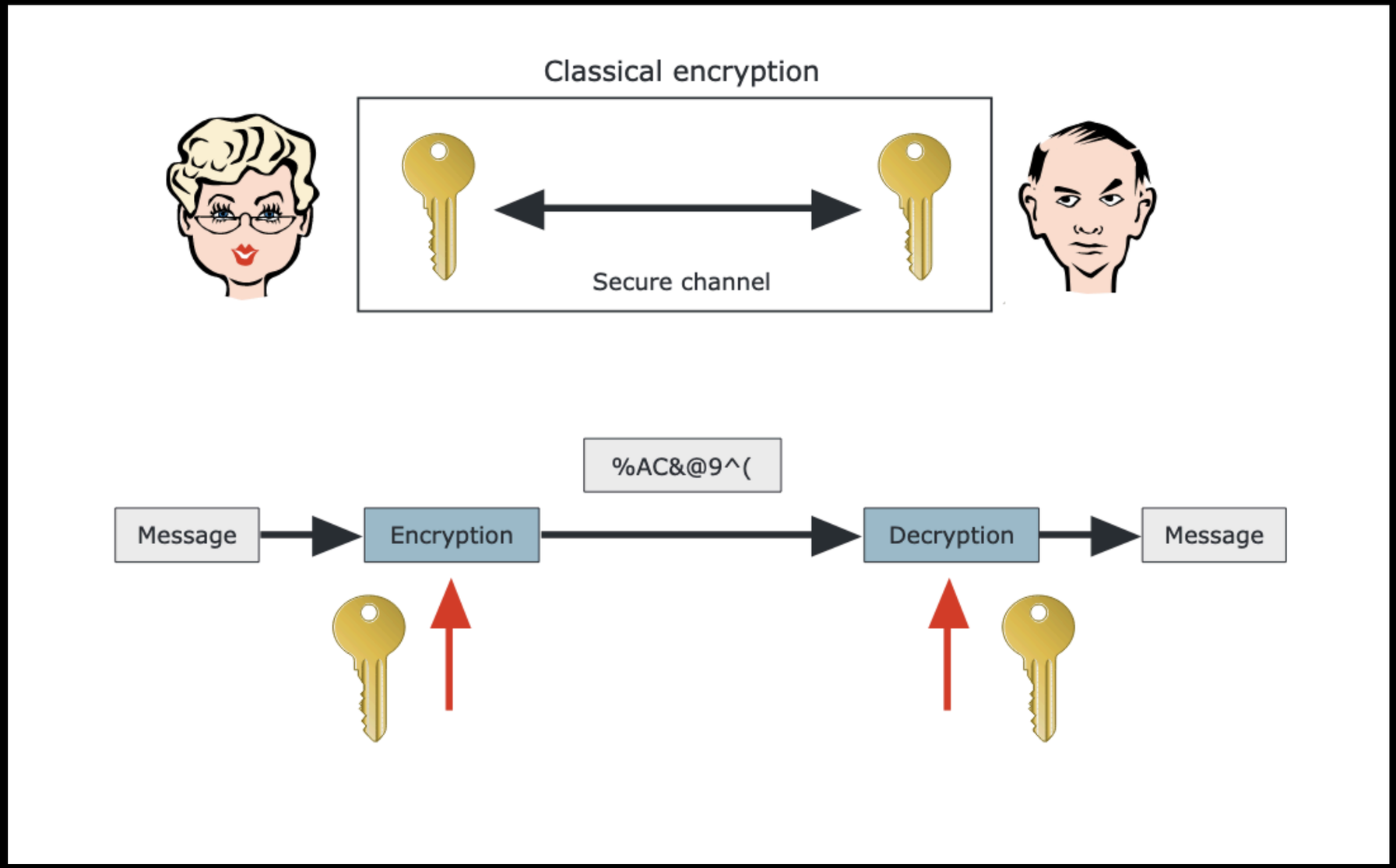
What is Symmetric Cryptography?

Think: One lock, one key — shared between trusted parties.

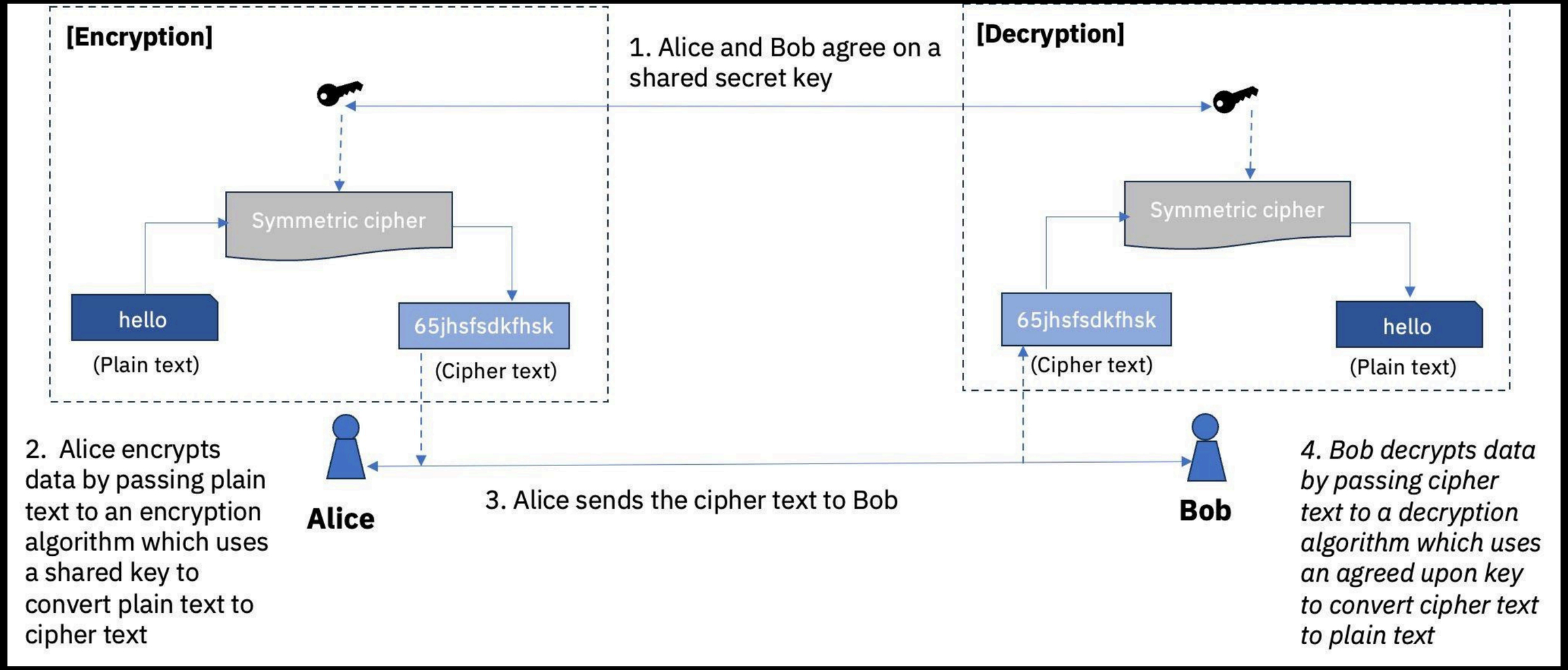
- Both encryption and decryption use the same secret key
- Fast, lightweight, and great for bulk data
- Used in: File encryption, Wi-Fi, ZIPs, and even disk drives



Symmetric Cryptography



A more formal Symmetric Cryptosystem



So what are challenges of this system?

Symmetric Key Cryptography

Implementing a secure symmetric key cryptosystem involves two main tasks:

- Employing a robust symmetric key encryption algorithm resistant to cryptographic attacks.
- Ensuring confidentiality in the distribution and management of secret keys.

So if there is increased risk why use symmetric key cryptography?

Advantages of SKC

- The number one reason why a symmetric key would be used over an asymmetric key for data **encryption is speed.**
- Symmetric key encryption and decryption is done quicker and with **less processing power**.
- Because i**t’s built in**. Many vendors use symmetric key technology within their products to protect sensitive data and operations.
- The **keys always remain local** and there is no need for an entity to exchange or move those keys.

Now lets get into the types of SKC

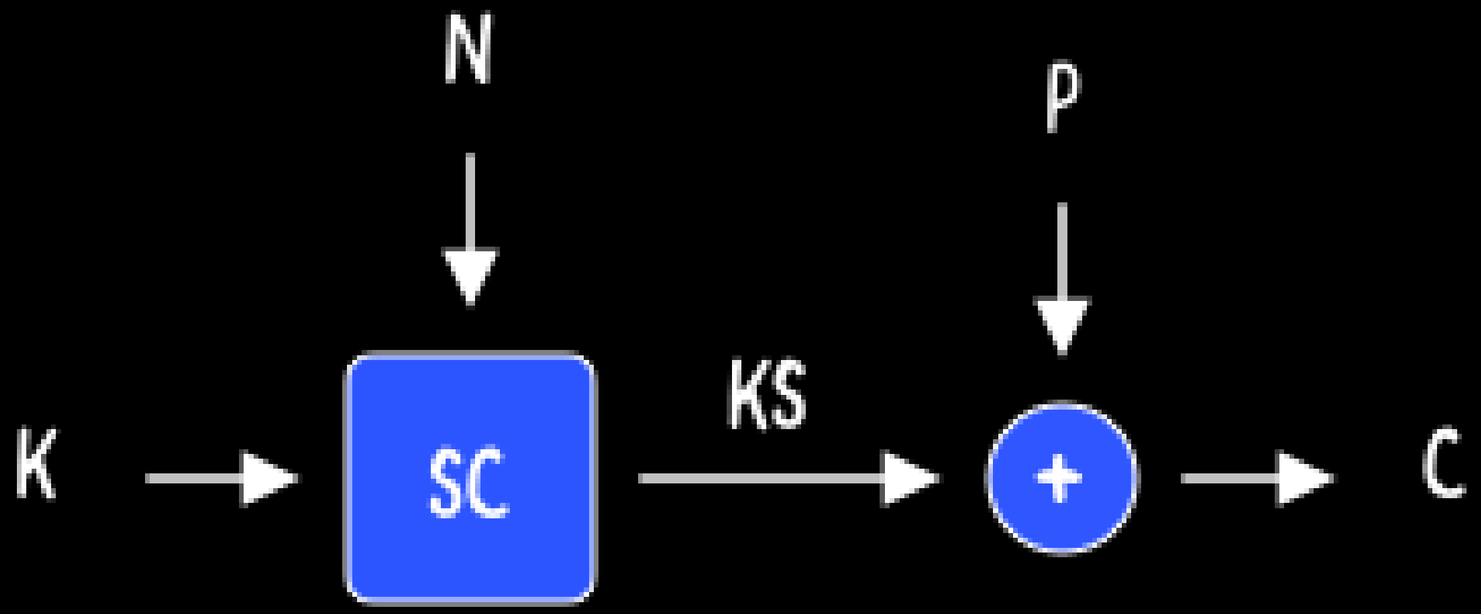
Stream Ciphers

- A stream cipher is an encryption technique that works bit by bit to transform plain text into code that's unreadable to anyone without the proper key.
- Stream ciphers are linear, so the same key both encrypts and decrypts messages.
- While cracking them can be difficult, hackers have managed to do it.
- For that reason, experts feel stream ciphers aren't safe for widespread use.

How do they work?

- A stream cipher encrypts a continuous string of binary digits by applying time-varying transformations on plaintext data.
- It works bit-by-bit, using keystreams to generate ciphertext for arbitrary lengths of plain text messages.
- The cipher combines a key (128/256 bits) and a nonce digit (64-128 bits) to produce the keystream — a pseudorandom number XORed with the plaintext to produce ciphertext.
- While the key and the nonce can be reused, the keystream has to be unique for each encryption iteration to ensure security.

How do they work?



Examples of Stream Ciphers

Rivest Cipher (RC4)

- RC4/ARC4/ARCFOUR is a fast, simple encryption algorithm developed in 1987 to implement byte-by-byte encryption using 64 or 128 bits long keys.

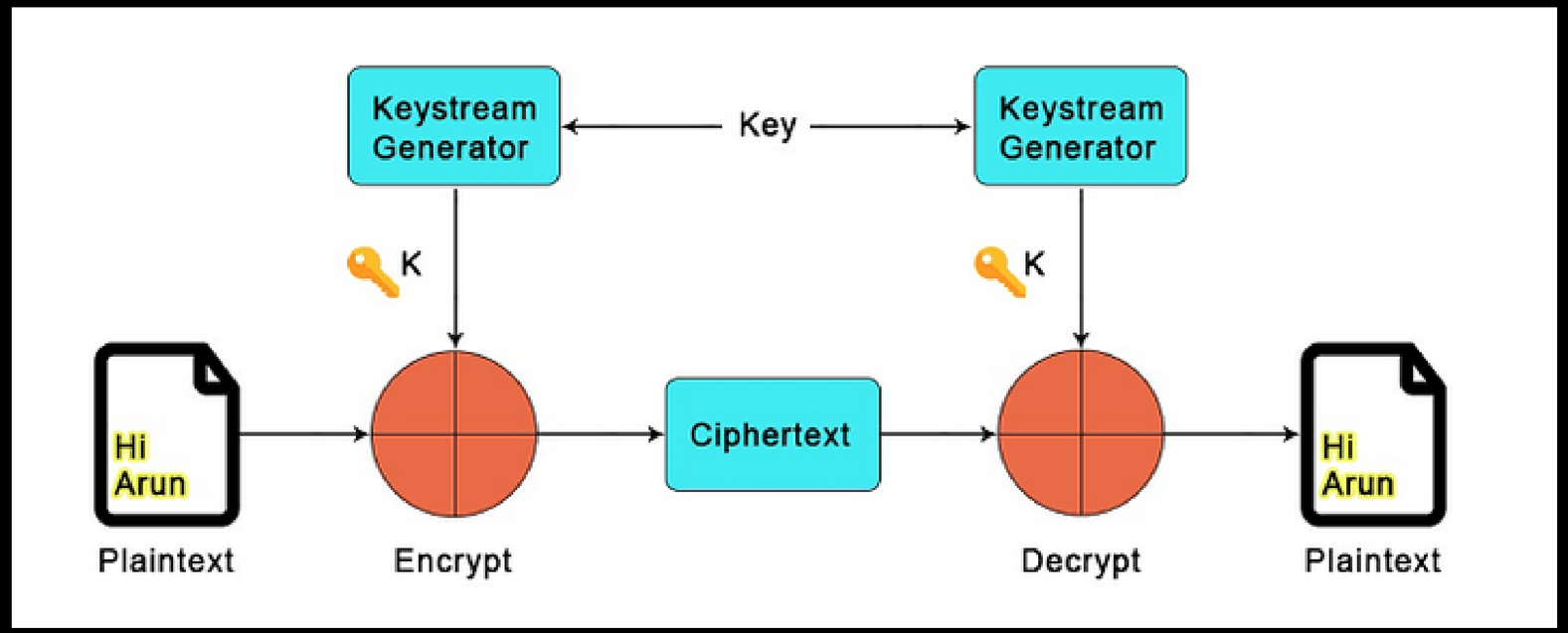
Salsa20

- Salsa20 is an efficient, modern encryption cipher that relies on an expansion function to produce the encryption keystream.
- Other examples of stream ciphers include PANAMA, Scream, Rabbit, HC-256, and Grain, among others.

Why Stream Ciphers?

Stream ciphers come with plenty of benefits, including:

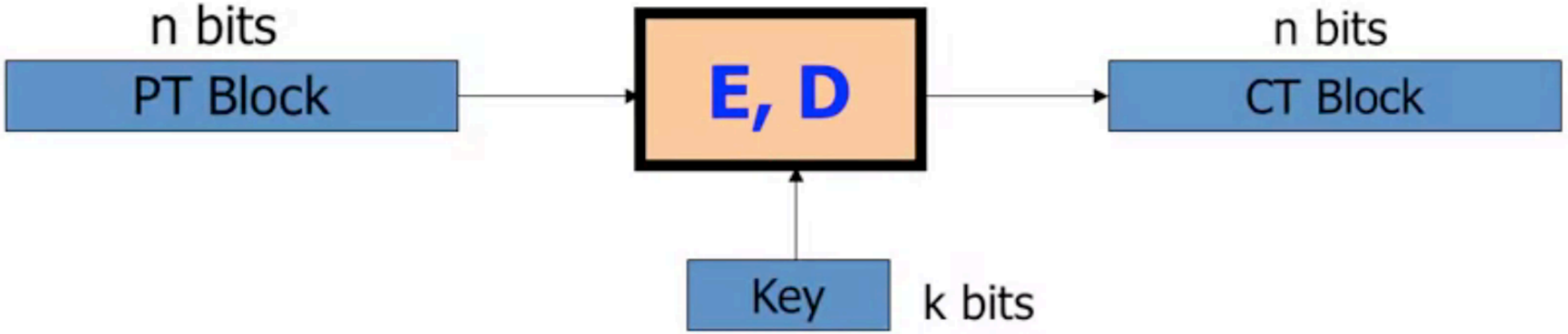
- Speed
- Low complexity
- Serial nature
- Ease of use



Block Ciphers

- A block cipher is 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.
- For 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.

Block ciphers: crypto work horse



Canonical examples:

1. 3DES: n= 64 bits, k = 168 bits
2. AES: n=128 bits, k = 128, 192, 256 bits

Characteristics of Block Ciphers

- **Confusion:** Confusion is the characteristic whereby each bit in the ciphertext depends on multiple bits of the secret key. It ensures that a small change in the secret key modifies almost all the bits of the ciphertext, obscuring the relationship between the ciphertext and the secret key.
- **Diffusion:** Diffusion is the characteristic whereby flipping a single bit in the plain text should modify roughly half the bits in the ciphertext and vice versa. Diffusion hides statistical relationships between the plain text and ciphertext. Ciphers with adequate diffusion satisfy the so-called avalanche criteria of cryptography.

Block Cipher Schemes

Block ciphers have many schemes to operate. Some of the widely used and popular ones are as follows:

- DES: Digital Encryption Standard. It’s broken and no more used.
- Triple DES: Repeated DES. Much stronger algos are available than this.
- AES: Advanced Encryption Standard.
- Serpent: Has block size of 128 bits and keys of length 128,196 or 256 bits. Slower but very secure than other block ciphers.
- TwoFish: With a block size of 128 bits, it is based on an earlier block cipher called Blowfish which uses a block of 64 bits

Difference between the two types

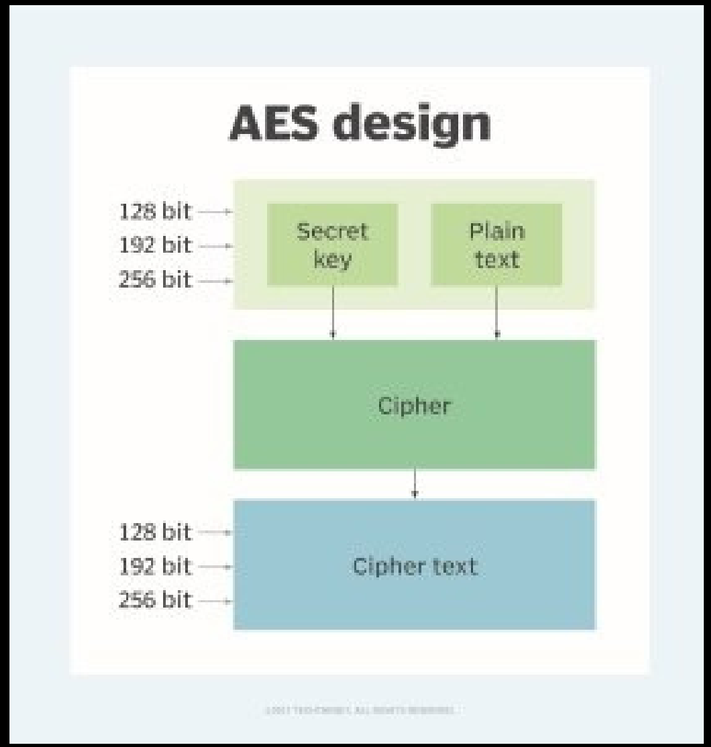
S.NO	Block Cipher	Stream Cipher
1	Block Cipher Converts the plain text into cipher text by taking plain text’s block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.
2	Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
3	The complexity of block cipher is simple.	While stream cipher is more complex.
4	Block cipher Uses confusion as well as diffusion.	While stream cipher uses only confusion.
5	In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.
6	The algorithm modes which are used in block cipher are ECB (Electronic Code Book) and CBC (Cipher Block Chaining).	The algorithm modes which are used in stream cipher are CFB (Cipher Feedback) and OFB (Output Feedback).
7	Block cipher works on transposition techniques like rail-fence technique, columnar transposition technique, etc.	While stream cipher works on substitution techniques like Caesar cipher, polygram substitution cipher, etc.
8	Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.

Lets look at some code to understand DES and AES

The Rise of AES

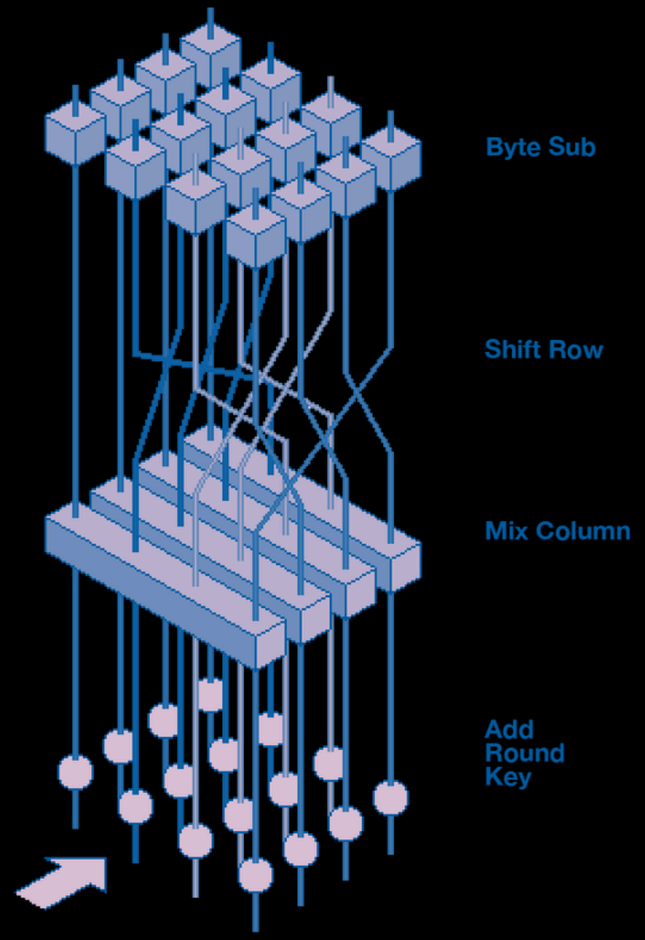
Fast, secure, and still unbroken — the king of symmetric ciphers.

- Advanced Encryption Standard (AES) — adopted in 2001.
- Replaced DES (outdated & weak).
- Based on Rijndael algorithm by Vincent Rijmen & Joan Daemen.
- Supports 128, 192, and 256-bit keys.



AES: The Transformation Process

- SubBytes → Non-linear substitution.
- ShiftRows → Rearranges data.
- MixColumns → Diffuses info across bytes.
- AddRoundKey → Combines with secret key.



What lessons do we take back from this?

Hands on for implementing the same