SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 2:

Symmetric Cryptography

Module 1 - Background of Classic Ciphers

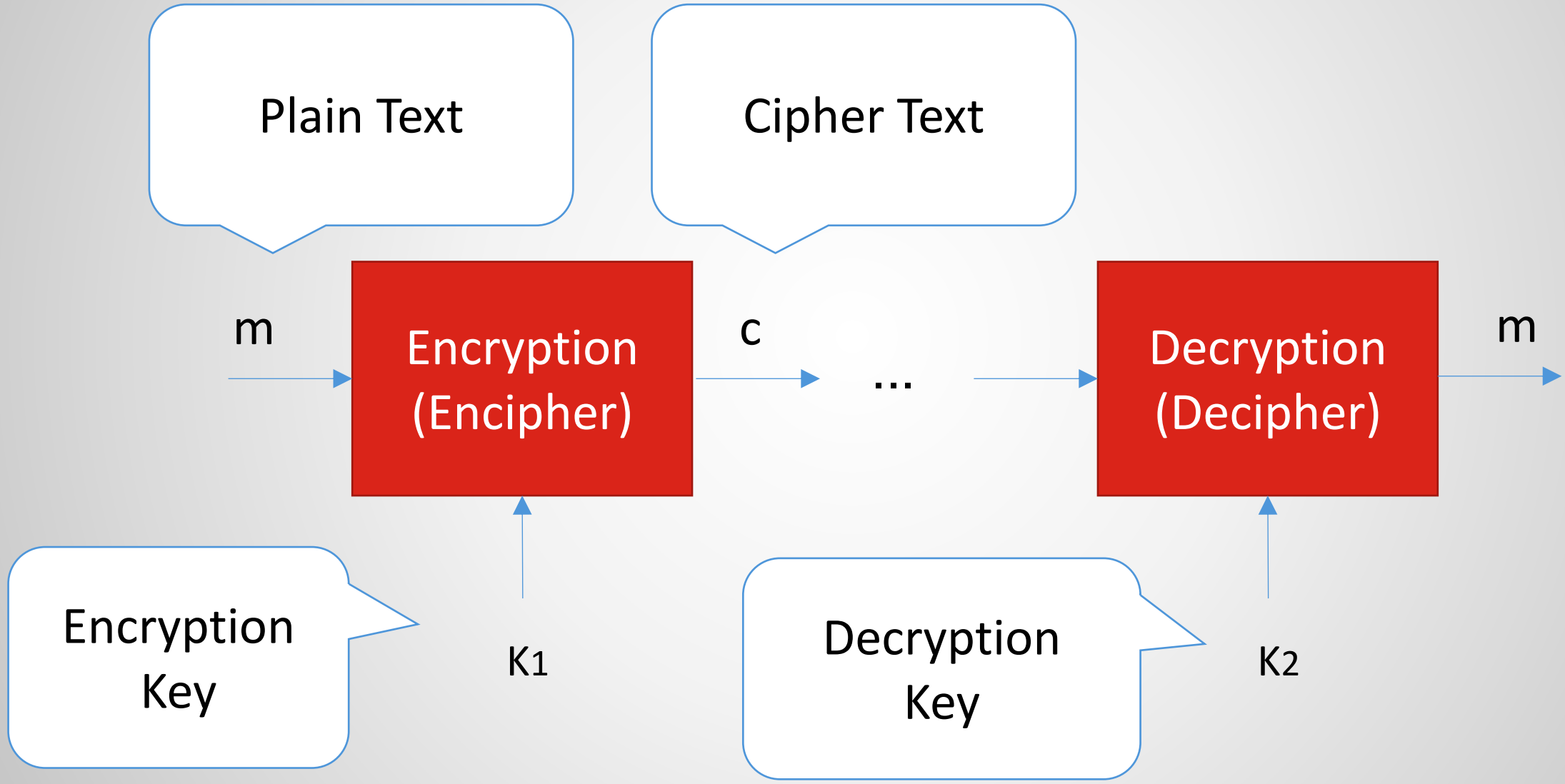
Cryptography is Found Everywhere

- Secure Communication
  - web traffic: HTTPS
  - wireless traffic: 802.11i WPA2 (and WEP), GSM, Bluetooth
- Secure File Systems
  - Encrypting File System (EFS) of Microsoft NTFS
  - Trucrypt, TPM
- DVD/Blue-ray
  - CSS
  - AACS

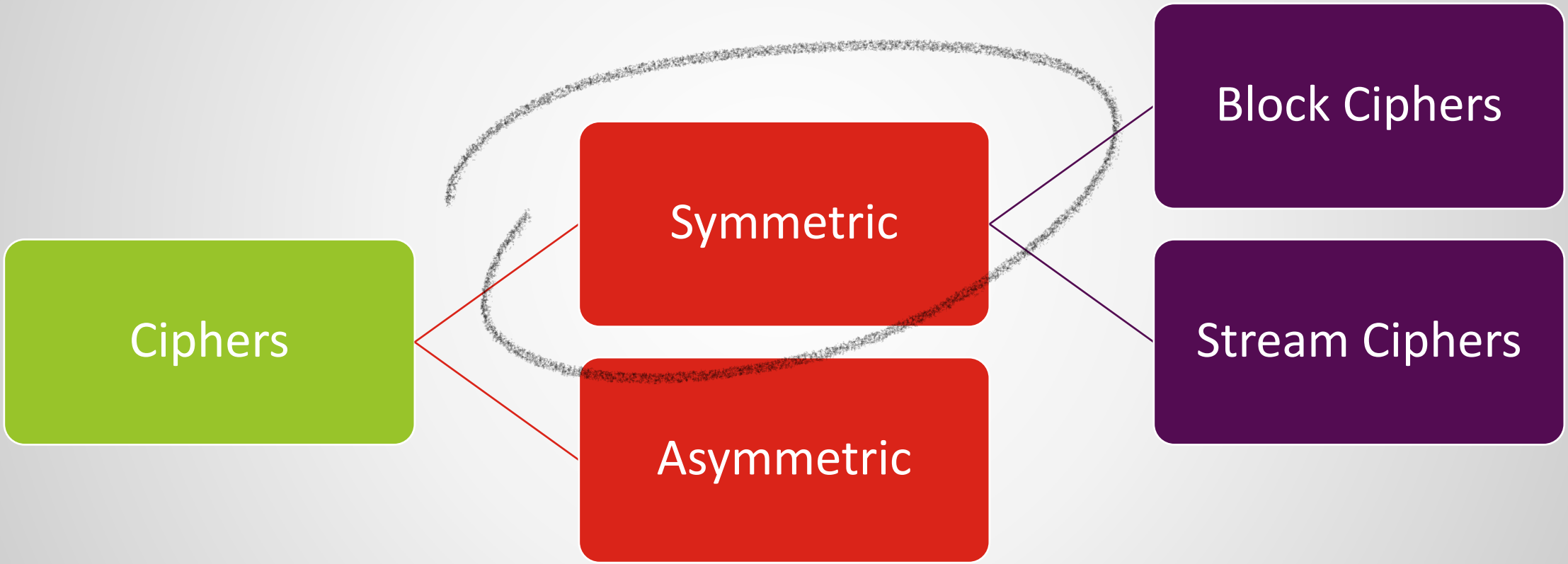
Broken

- Digital Signature, Banking, etc.
  - Smart Cards
  - Kerberos

Do You Remember This?



Classification of Ciphers



Some Classic Ciphers

- Generic Substitution Cipher

$$E_K(\text{"bcza"}) = \text{"what"}$$

$$D_K(\text{"what"}) = \text{"bcza"}$$

K =

Plain Text	Cipher Text
a	-> t
b	-> w
c	-> h
:	
z	-> a

Caesar Cipher

- Caesar Cipher
  - Shifts the plain text by 3 to create the cipher text

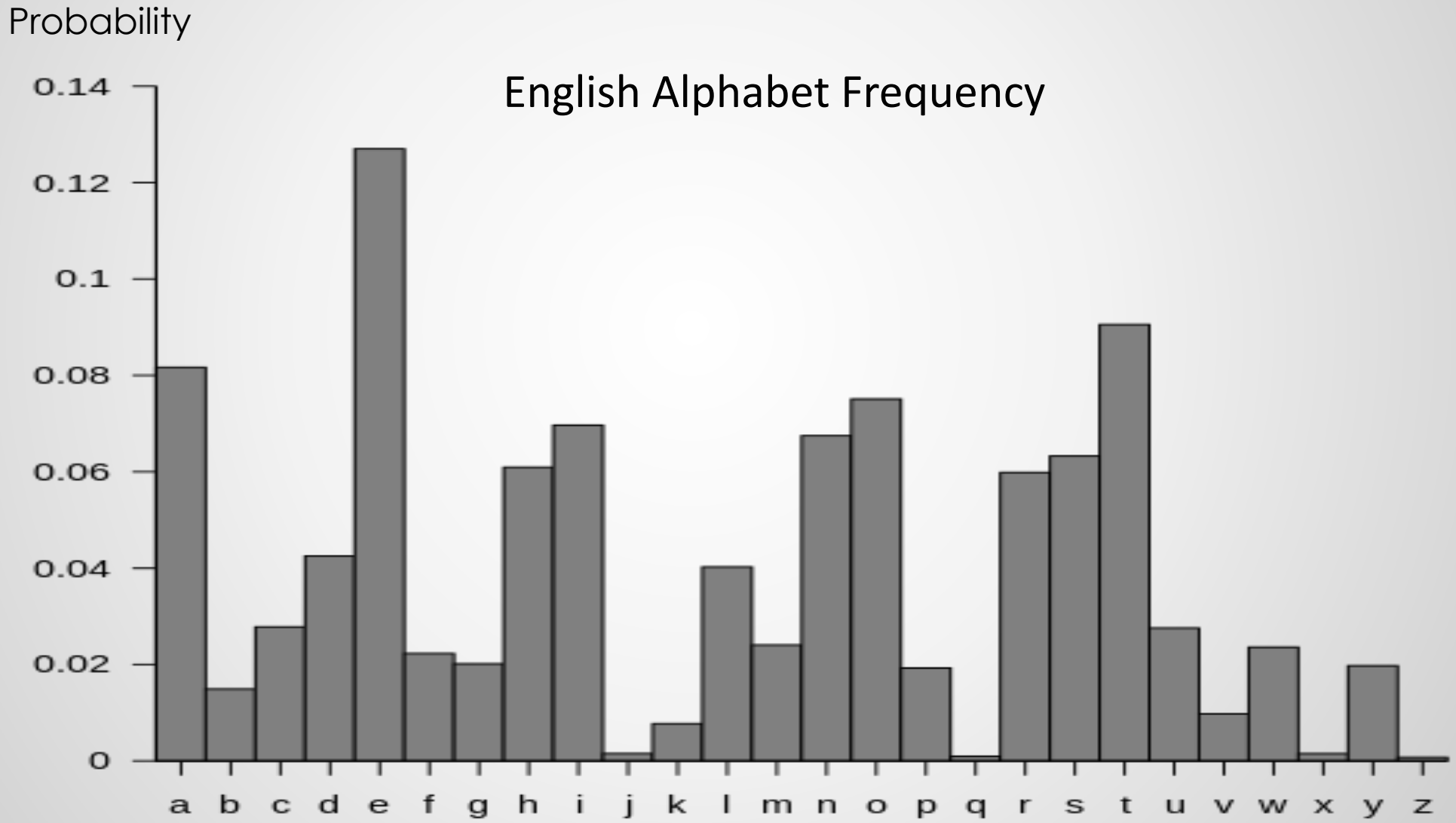
$$c = m + k \mod 26 \;;\; k=3$$

K =

Plain Text	Cipher Text
a	-> d
b	-> e
c	-> f
:	
z	-> c

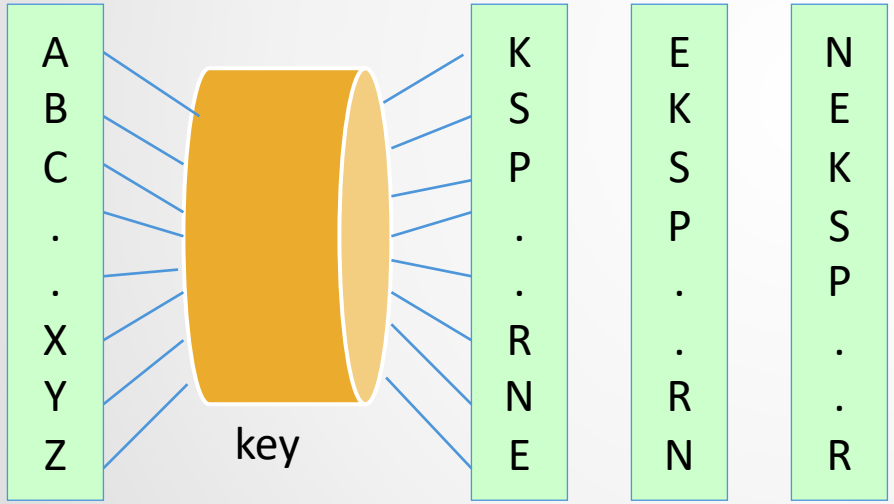
As an attacker, if we know that the algorithm is Caesar with a simple shift in letters, we need to only test 26 (actually 25) cases to find the key.

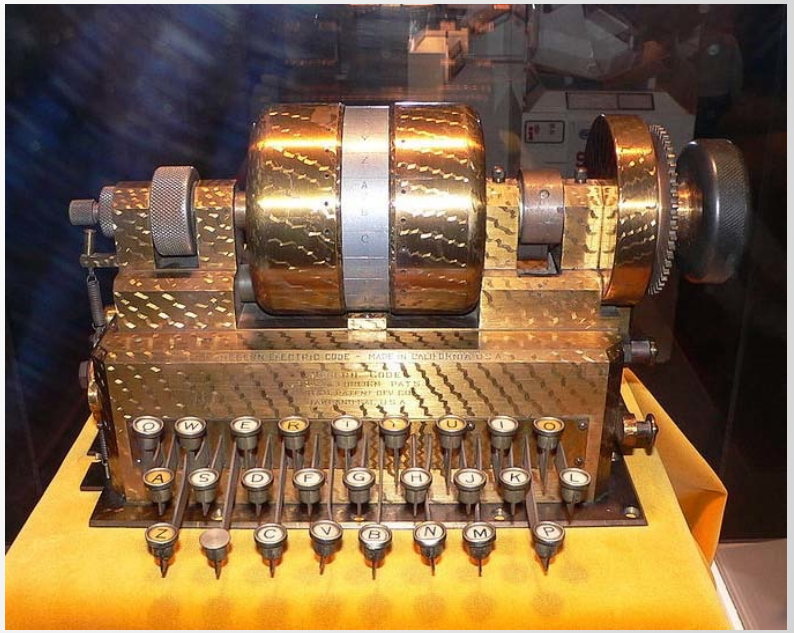
Frequency of Letters



Mechanical Ciphers (1870-1943)

The Hebern encryption machine (one rotor)

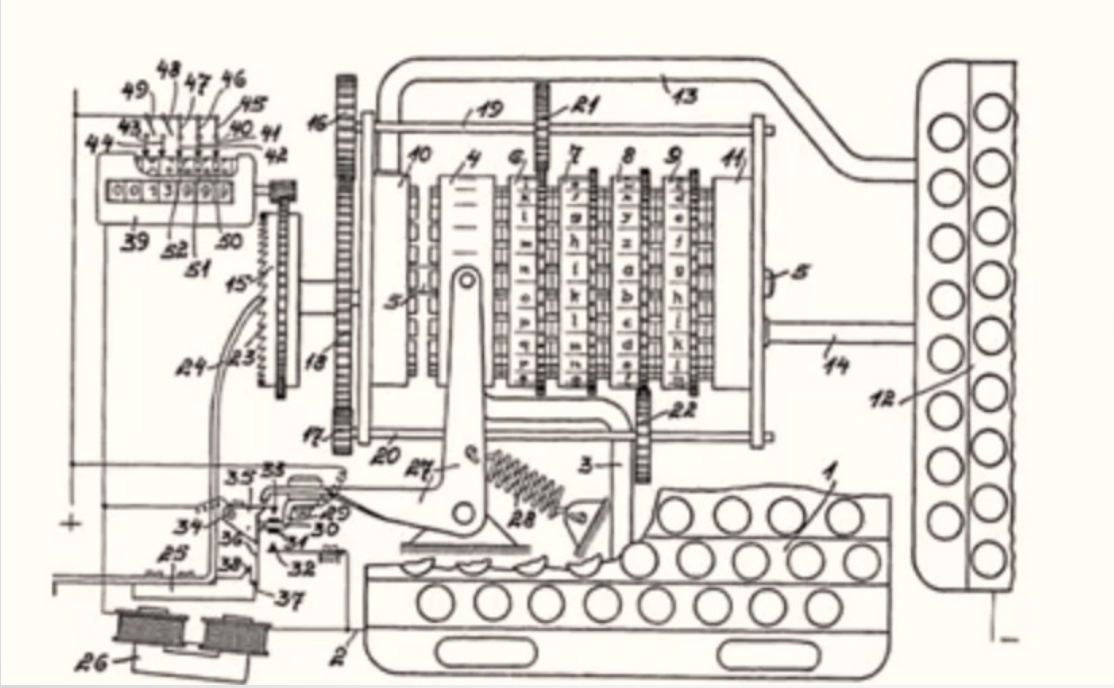




(Boneh, Stanford)

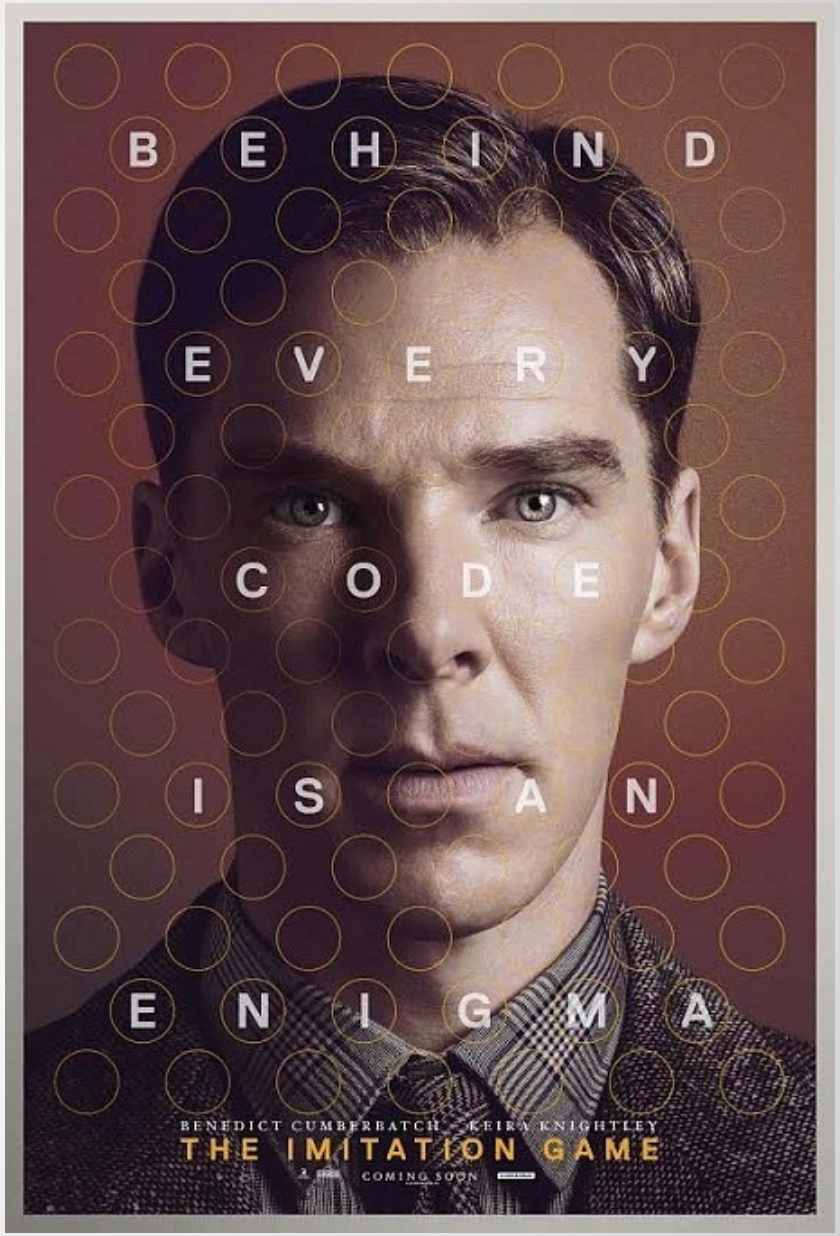
Mechanical Ciphers (1870-1943)

The Enigma (3 to 5 rotors)

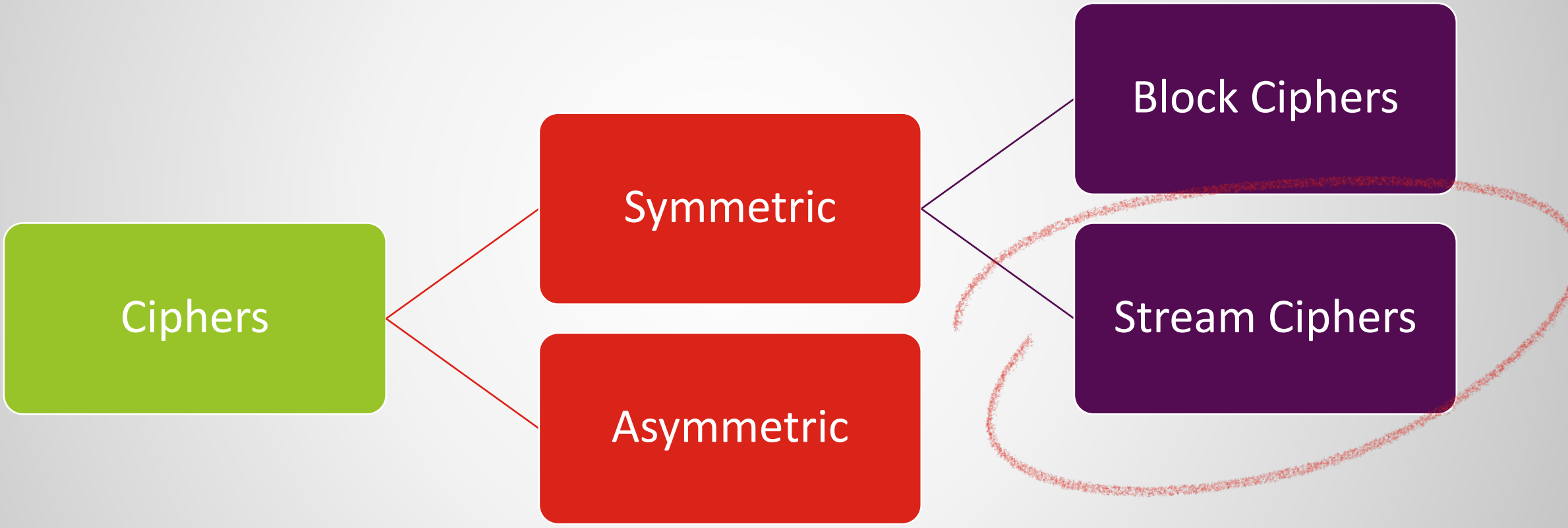


Key space (combinations) for a 4-rotor machine = $26^4 = 2^{18}$


SPECIAL EDITION
DOUGRAY SCOTT
KATE WINSLET
JEREMY NORTHAM
SAFFRON BURROWS
ENIGMA
"It's a Brilliant Film!"
Roger Ebert
DVD

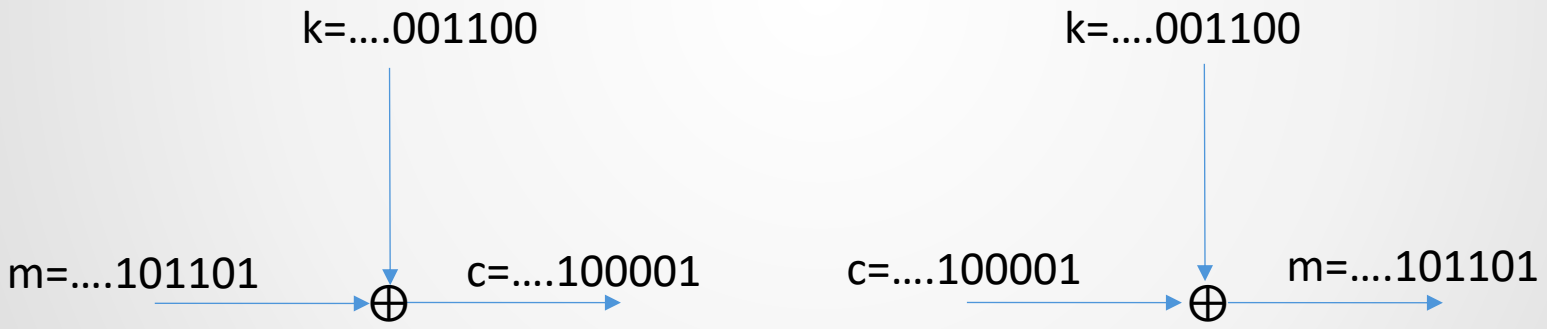

BEHIND
EVERY
CODE
IS AN
ENIGMA
BENEDICT CUMBERBATCH KEIRA KNIGHTLEY
THE IMITATION GAME
COMING SOON

Classification of Ciphers



Steam Cipher - One Time Pad

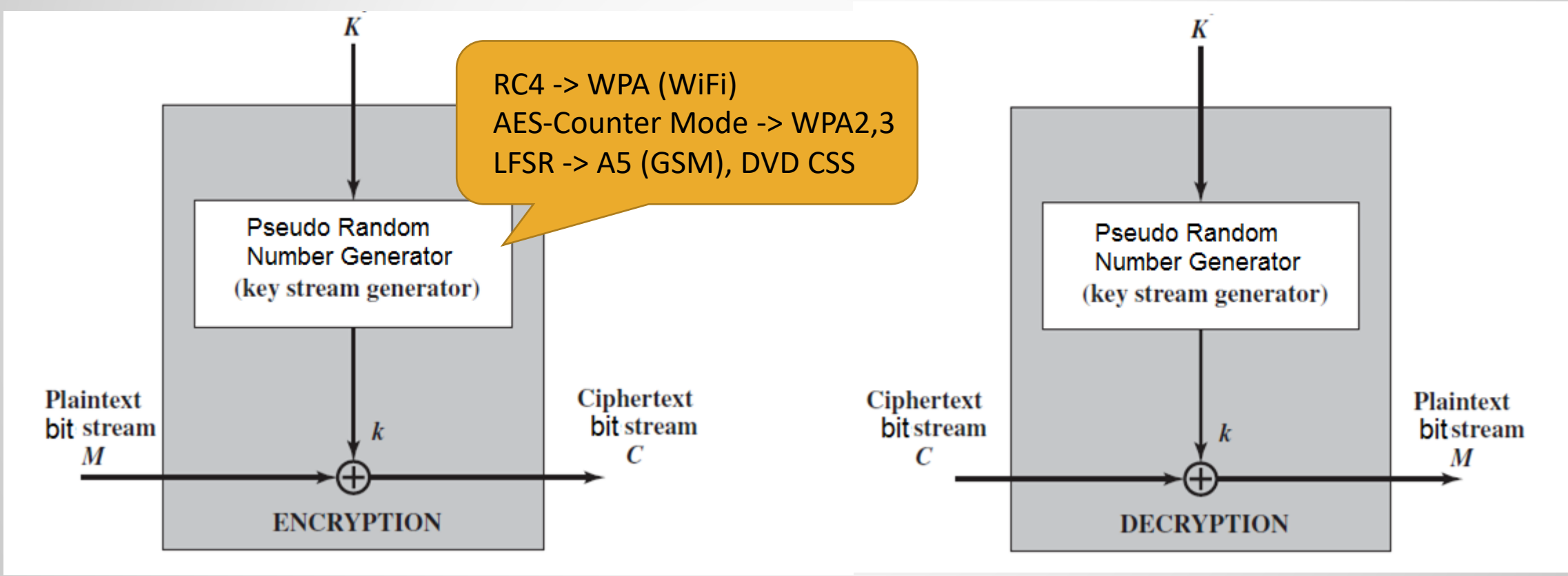
Stream ciphers, as the name says, encrypt and decrypt streams of data, usually in the form of bits. In the most basic form (which is called one time pad), key is a long string of bits, which is XORed one by one with the bits of the plaintext. A similar XOR operation at the receiver unmasks the ciphertext and gets the plaintext out.



Large key length renders it useless in practice

Stream Cipher Model

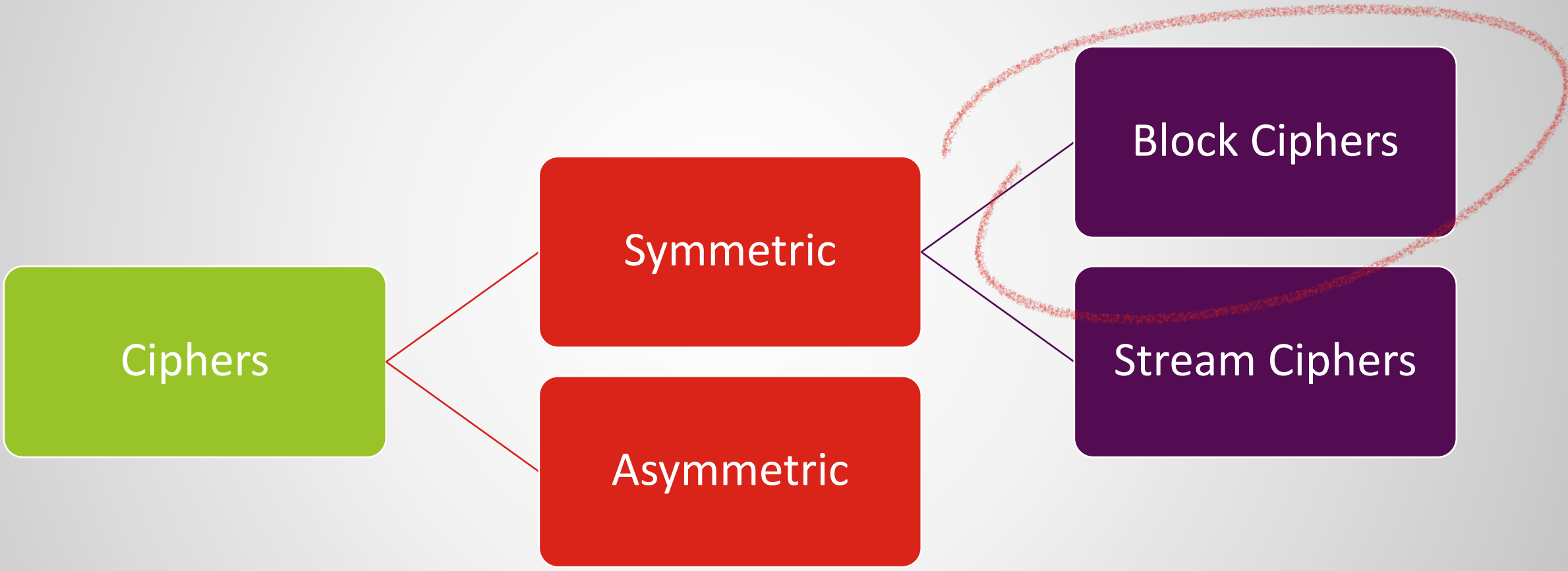
From a small seed (a master key), and by using a pseudo random number generation algorithm, a long sequence of bits is generated. These bits will be XORed with the plaintext to create the cipher text. A similar operation at the receiver undoes the encryption and gives the plaintext back.



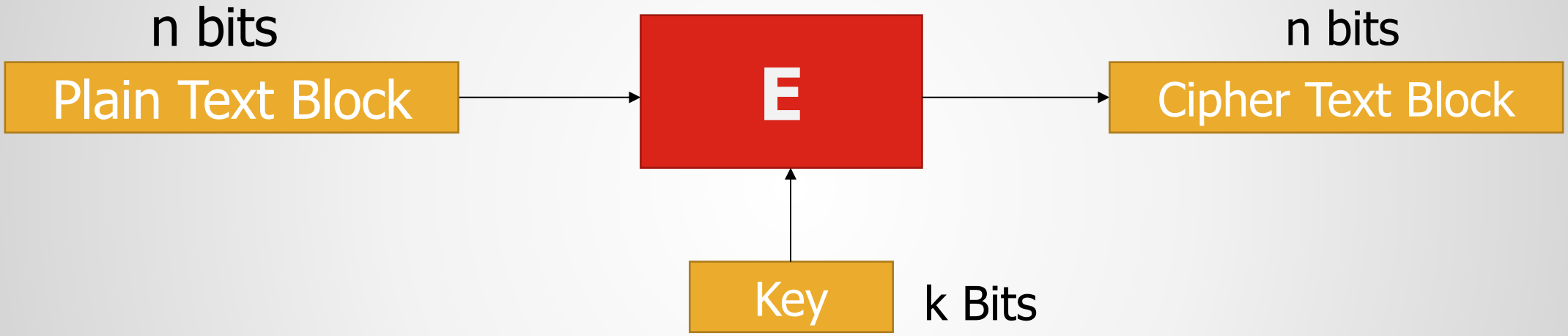
RC4 -> WPA (WiFi)
AES-Counter Mode -> WPA2,3
LFSR -> A5 (GSM), DVD CSS

(Stallings)

Classification of Ciphers



Block Ciphers Model



Example:

1. DES (Data Enc. Standard): n= 64 bits, k = 56 bits
2. AES (Adv. Enc. Standard): n=128 bits, k = 128, 192, 256 bits

What Comes Next …

- We learned about different families of cryptosystems.
- In the next video, we will focus on symmetric encryption and decryption algorithms.

See you in the next video …