CS489/689
Privacy, Cryptography, Network and Data Security

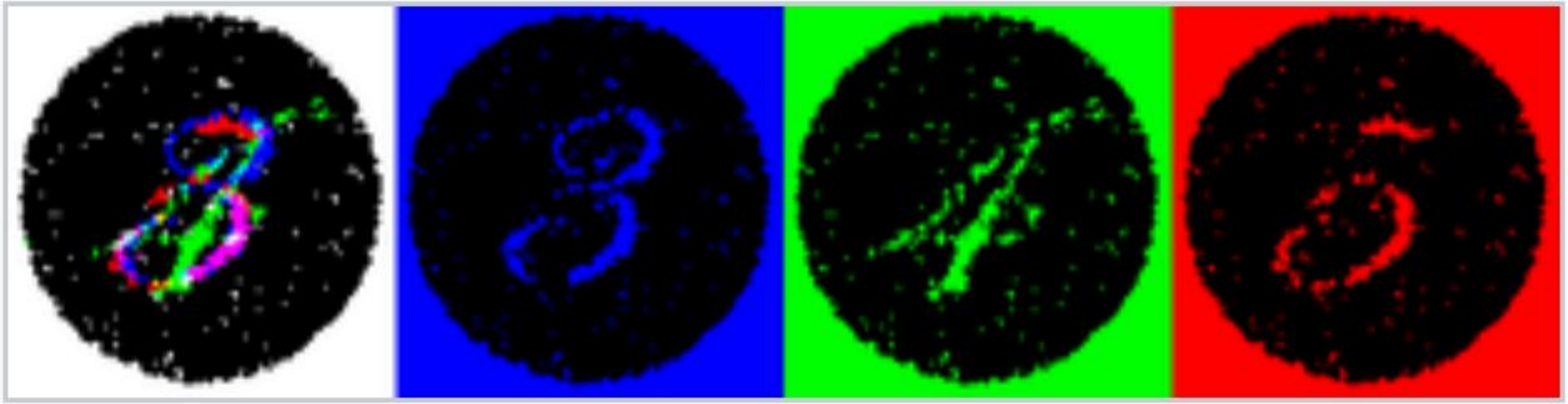
Winter 2023, Tuesday/Thursday 8:30-9:50am

Learning Outcomes

- Identify attack techniques and apply them (cryptanalysis)
- Explain building blocks of modern cryptography
- Explain how modern cryptography properties arose

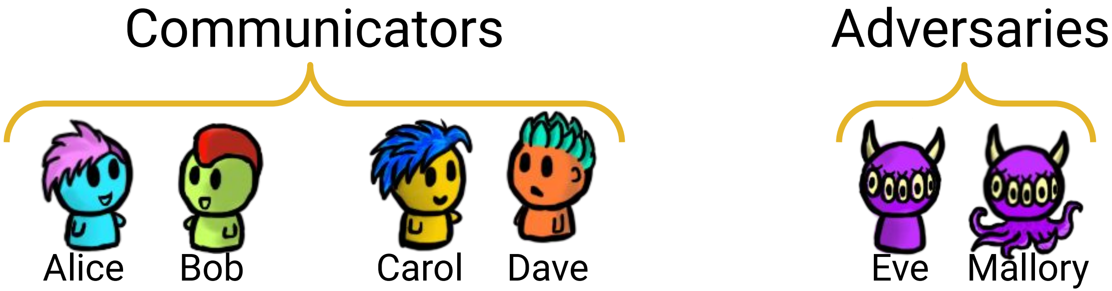
Goal: Basically, know what cryptography tools exist and how to securely use them. <u>Build a foundation of primitives</u> for more complicated "applied cryptography" later.

Steganography- Secretly "hidden" messages



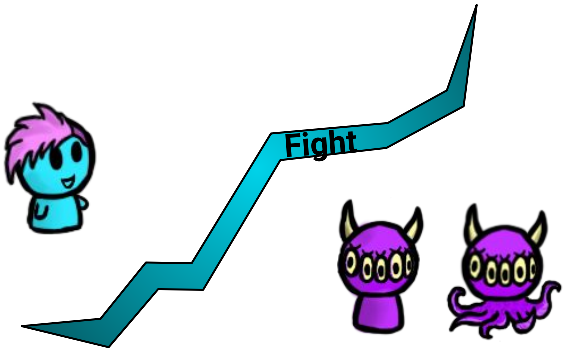
The same image viewed by white, blue, green, and red lights reveals different hidden numbers.

Cryptography - Writing “secret” messages

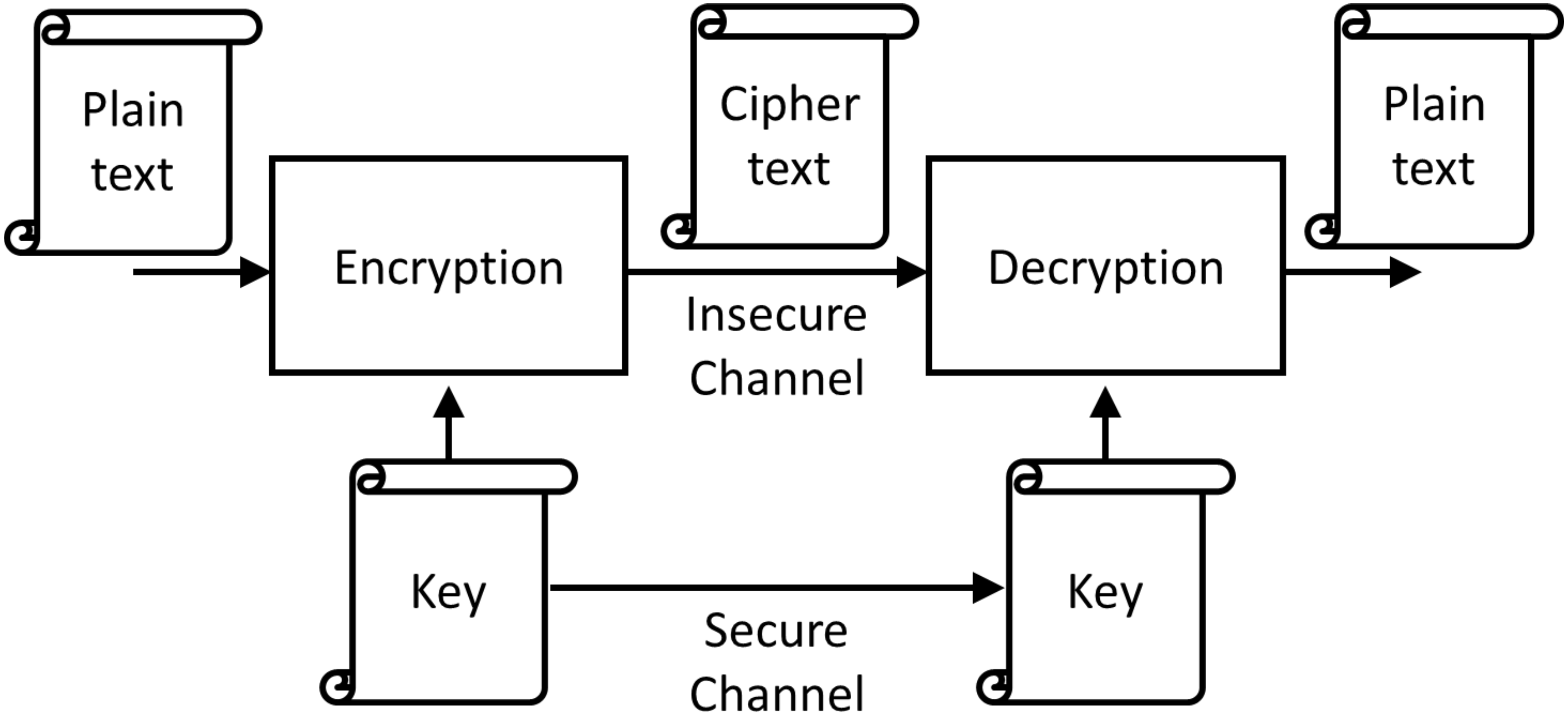


Remember CIA? Different A for Crypto Power

- Confidentiality, prevent Eve **reading** Alice's messages
- Integrity, prevent Mallory from **changing** Alice's messages
- Authenticity, Prevent Mallory from **impersonating** Alice



Cryptography - Path for Secret Messages



Historical Ciphers: Example One

FUBSWRJUDSKB

CRYPTOGRAPHY

Caesar Cipher

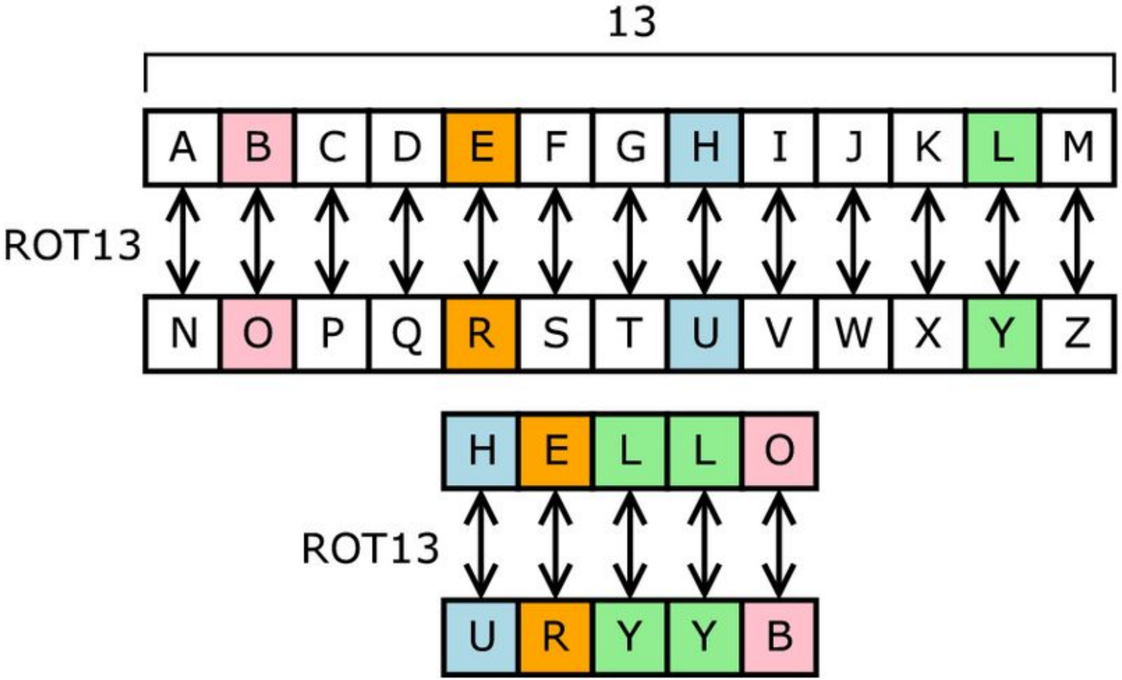


Image source: wikipedia

Shift and Substitution Ciphers

Replace symbols (letters) by others

- Using a rule e.g., $y = x + 3 \pmod{26}$, Caesar‘s cipher Key: 3
- Using a table e.g, Key: table

Cryptanalysis - Analyzing “secret” messages

Mwahaha

We will learn the secretsssss.

Historical Ciphers: Example Two

gsrh xlfihv rh zylfg xibkgltizksb uli gsv urihg gsivv dvvph. zmw gsvm zkkorvw xibkgltizksb uli kirezxb zmw hvxfirgb lu wzgz.

English Frequency

A	11.7%
B	4.4%
C	5.2%
D	3.2%
E	2.8%
F	4%
G	1.6%
H	4.2%
I	7.3%
J	0.51%
K	0.86%
L	2.4%
M	3.8%

N	2.3%
O	7.6%
P	4.3%
Q	0.22%
R	2.8%
S	6.7%
T	16%
U	1.2%
V	0.82%
W	5.5%
X	0.045%
Y	0.76%
Z	0.045%

Historical Ciphers: Example Two

gsrh xlfihv rh zylfg xibkgltizksb uli **gs**v urihg **gs**ivv dvvph. zmw **gs**vm zkkorvw xibkgltizksb uli kirezxb zmw hvxfirgb lu wzgz.

Historical Ciphers: Example Two

gsrh xlfihv rh zylfg xibkgltizksb uli **gs**v urihg **gs**ivv dvvph. zmw **gs**vm zkkorvw xibkgltizksb uli kirezxb zmw hvxfirgb lu wzgz.

This course is about cryptography for **th**e first **th**ree weeks. And **th**en applied cryptography for privacy and security of data.

Kerckhoff Principle

The security of a cryptosystem should solely depend on the secrecy of the key, but never on the secrecy of the algorithms.

Historical Ciphers: Example Three

LECTURE SECURITY AND CRYPTOGRAPHY I

↓

LENGECDRCUCATRRPUIYHRTPYEYTISAO

Historical Ciphers: Example Three

LECTURES

ECURITYA

NDCRYPTO

GRAPHYI

↓

LENGECDRCUCATRRPUIYHRTPYEYTISAO

Historical Ciphers: Example Three

Shannon's maxim!!!! (design assuming they'll learn the algorithm

LENGECDRCUCATRRRPUIYHRTPYEYTISAO

Shannon's Maxim and Kerkhoff's Principle Mean:

- Security shouldn't rely on the secrecy of the method
- Do use <u>public</u> algorithms with <u>secret</u> "keys"
- The adversaries target…is the key

Key: Easier to change a "short" key than your whole system.
(e.g., Recovery)

Unconditionally Secure: One-Time Pad

Message: x_0 x_1 x_2 … x_n

$\oplus$

Key: k_0 k_1 k_2 … k_n

$=$

Ciphertext: y_0 y_1 y_2 … y_n

Rule: $y_i = x_i + k_i \pmod 2$

Provably Security for One-Time Pad

<Ciphertext is uniformly distributed independent of the plaintext distribution>

x_i = 0 with probability p (x_i = 1: 1-p), k_i = 0 with probability 0.5 (k_i = 1: 0.5), y_i = 0 with probability:

$$p(y_i = 0) = p(x_i = 0)\, p(k_i = 0) + p(x_i = 1)\, p(k_i = 1)$$

$$= 0.5p + 0.5(1-p)$$

$$= 0.5$$

Provably Secure Con’t

Every ciphertext y can be decrypted **into every arbitrary plaintext** x using the key

$$\mathbf{k = yx}$$

Consequently the ciphertext cannot contain any information about the plaintext

Encryption is “deniable”

Act.

What if it is a many-time pad?

Key: K

$Ciphertext_1$= $message_1$ xor K = 1f0c001745150501590c0015

$Ciphertext_2$= $message_2$ xor K = 131c07060011540d0015070112

Your turn, goal: Learn the ciphertexts.

Hmmm…what do I know these are made of…and definitely contain?

What if it is a many-time pad?

Act.

Key: K

Ciphertex… 5

Cipherte… 12

FAQ:

- Submit the steps you used to learn (your almost algorithm).
- If you found the solution (messages), include that, else
  - Indicate how far you got and what ideas you had left for what to try next.

Hmmm…what do I know these are made of…and definitely contain?

Many-time pad? Messages Lack True Randomness

C_1

C_2

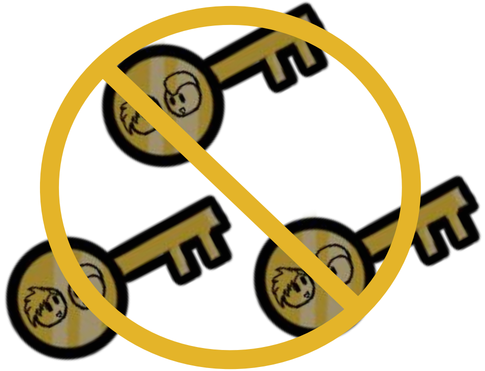
$C_1 \oplus C_2$

M_2

M_1

One-Time Pad - Conditions...

- Key as long as the message
- Key uniformly random
- Only used once



So...Cryptography?

- Simple substitution/transposition is computationally insecure
- One-Time Pad is inefficient over the secure channel

Goal: Securely communicate "a lot" of information on an insecure channel while requiring "limited" communication over a secure channel

Recap: A, B, C versus A and B and C

Substitution is insecure…

Transposition is insecure…

Key reuse using XOR (one-time pad) is insecure…

BUT

Repeat it often enough and it can be widely regarded as secure

Recap: A, B, C versus A and B and C

Substitution is insecure…

Transposition is in

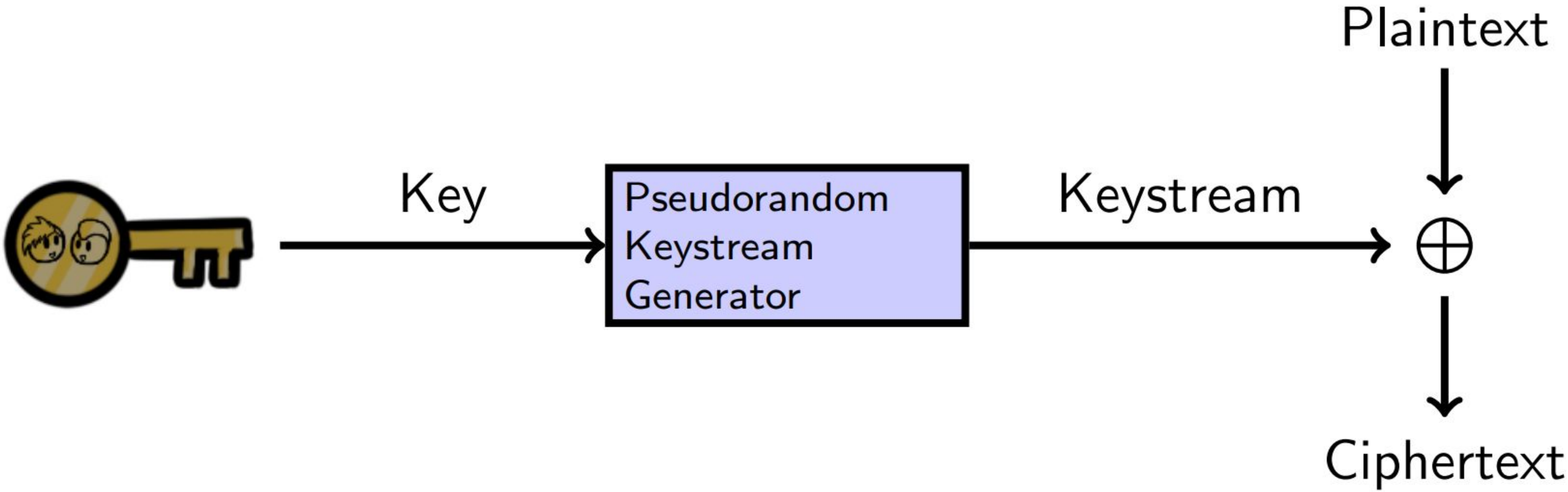
Key reuse … d) is insecure…

BUT

Repeat it often enough and it can be widely regarded as secure

Stream Ciphers and Block Ciphers

Stream Cipher?

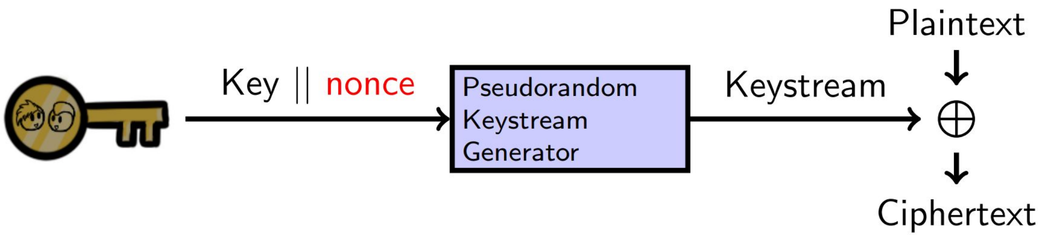


Fun(?) Facts:

- RC4 was the most common stream cipher on the Internet but deprecated.
- ChaCha increasingly popular (Chrome and Android), and SNOW3G in mobile phone networks.

Stream Ciphers Share Conditions with OTP

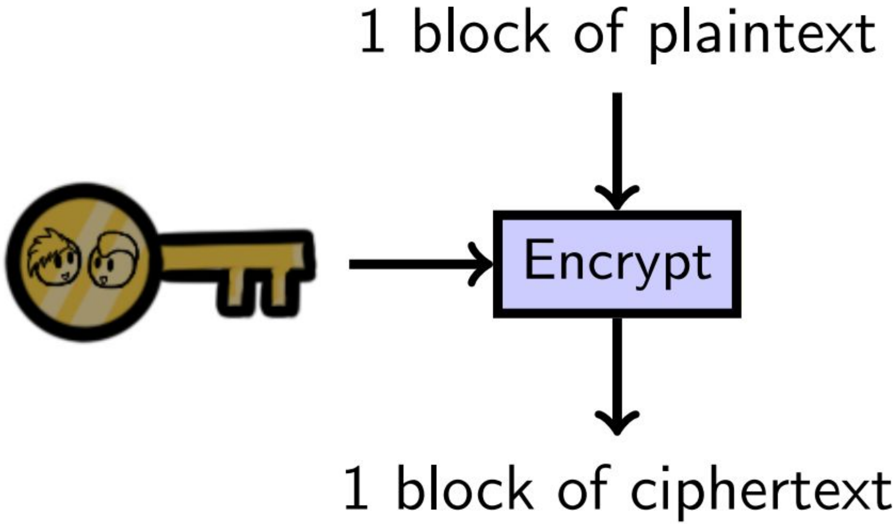
- Stream ciphers can be very fast
  - This is useful if you need to send a lot of data securely
- But they can be tricky to use correctly!
  - We saw the issues of re-using a key! (two-time pad)
  - Solution: concatenate key with nonce (we'll see more about nonces later)



Fun(?) Facts:

- WEP, PPTP are great examples of how not to use stream ciphers

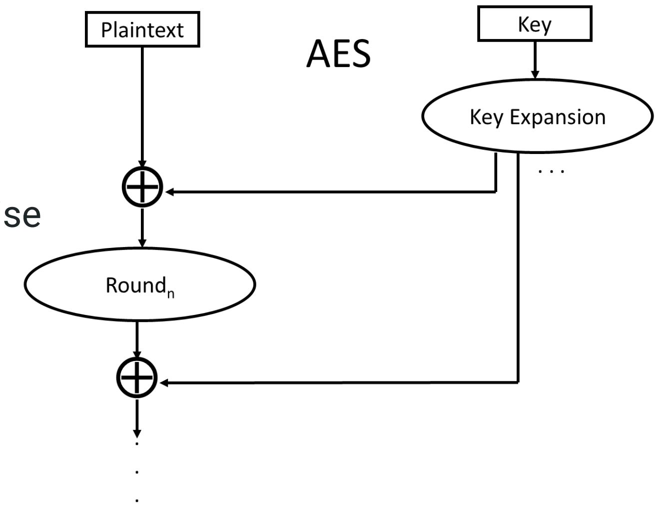
Bit by bit....do you have to?



Block ciphers!!!

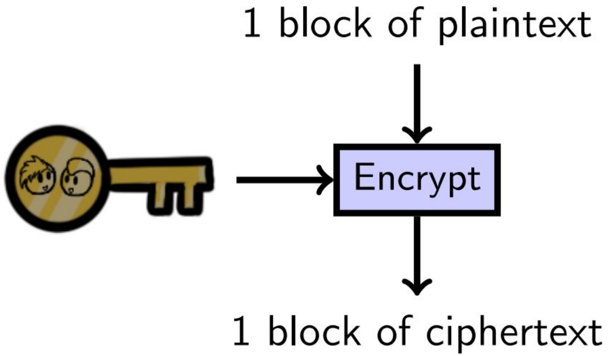
Block Ciphers

- Weakness of streams…one bit at a time?
    - What happens in a stream cipher if you change just one bit of the plaintext?
- Welcome, use of block ciphers
    - Block ciphers operate on the message one block at a time
    - Blocks are usually 64 or 128 bits long
- **AES**, the current standard
    - You better have a very…very good reason to choose otherwise

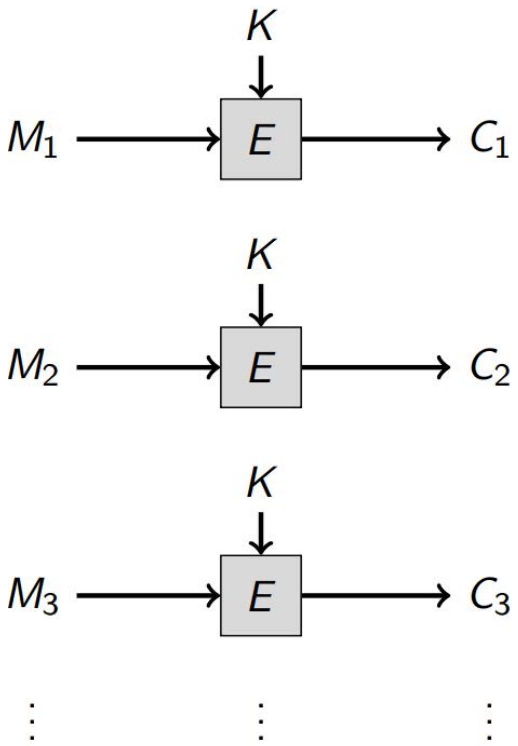


Two Catches with Block Ciphers

- Message is shorter than one block
  - padding
- Message is longer than a block
  - Modes of operation <new concept>

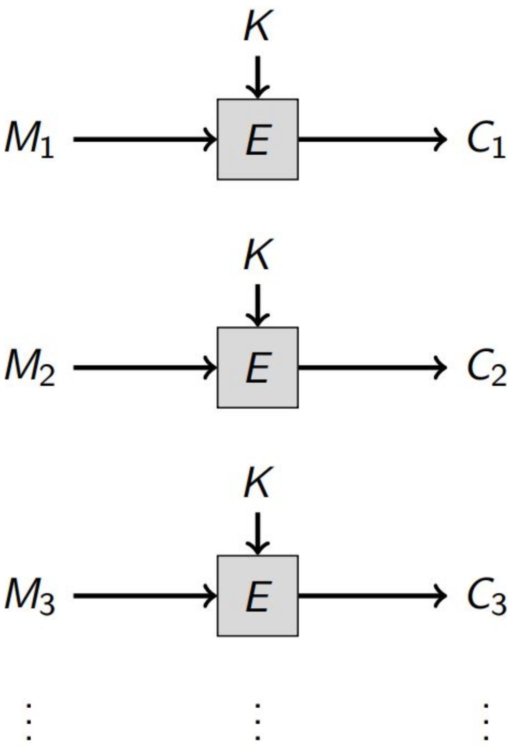


Block Ciphers and Modes of Operation: ECB Mode



- ECB: Electronic Code Book
- Encrypts each successive block separately

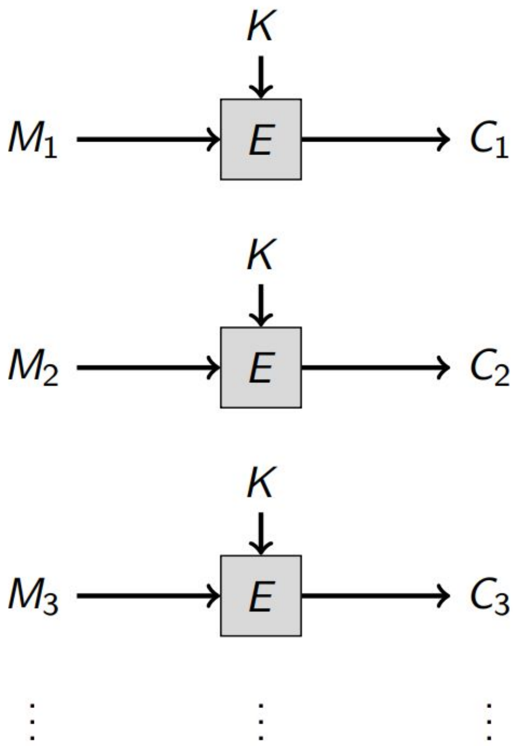
Block Ciphers and Modes of Operation: ECB Mode



- ECB: Electronic Code Book
- Encrypts each successive block separately

Q: What happens if the plaintext M has some blocks that are identical, $M_i = M_j$?

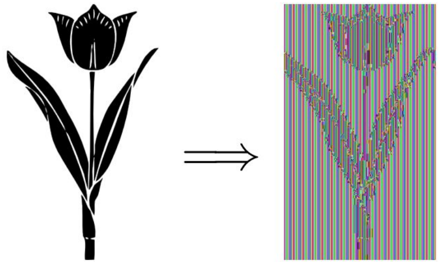
Block Ciphers and Modes of Operation: ECB Mode



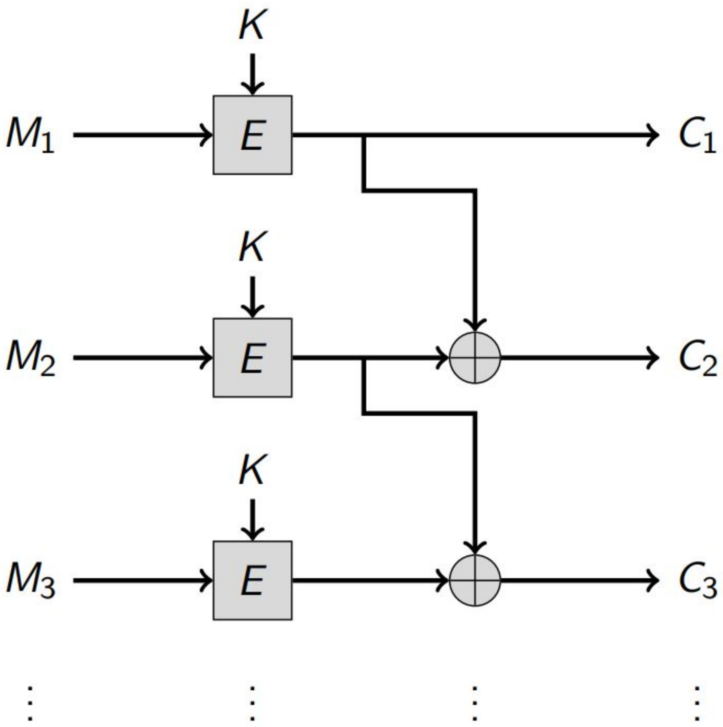
- ECB: Electronic Code Book
- Encrypts each successive block separately

Q: What happens if the plaintext M has some blocks that are identical, $M_i = M_j$?

A: $C_i = E_K(M_i)$, $C_j = E_K(M_j) \Rightarrow C_i = C_j$



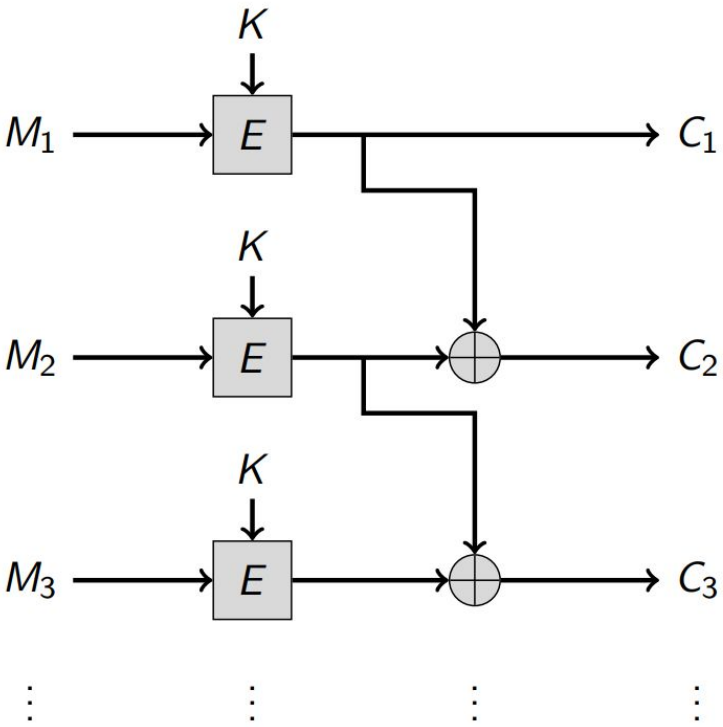
Attempt 1: Fixing ECB[1]



- Provide "feedback" among different blocks, to avoid repeating patterns…

Q: Fix repeating patterns? Are there other issues?

Attempt 1: Fixing ECB[1]

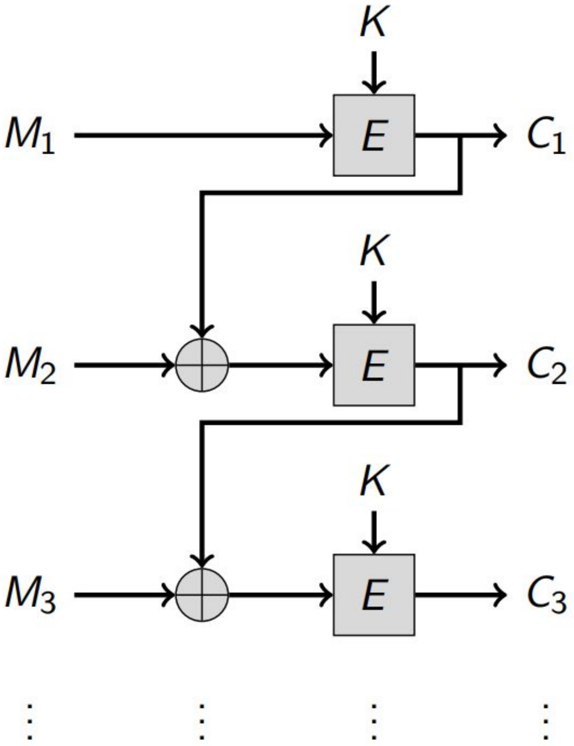


- Provide "feedback" among different blocks, to avoid repeating patterns…

Q: Fix repeating patterns? Are there other issues?

A: We can un-do the XOR <u>if we get all the ciphertexts</u>. This basically does not improve compared to ECB.

Attempt 2: ECB_2!!!

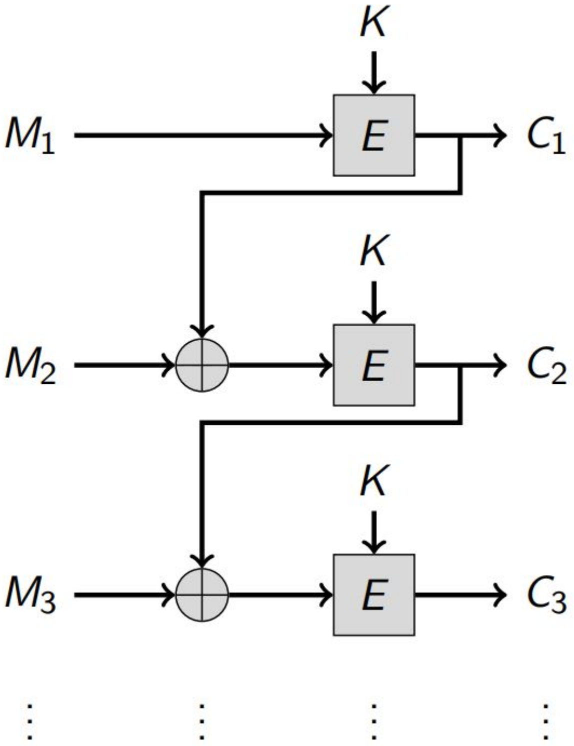


Q: Spot the difference?

Q: Is it fixed this time?

Q: Does this avoid repeating patterns among blocks?

Attempt 2: ECB_2!!!



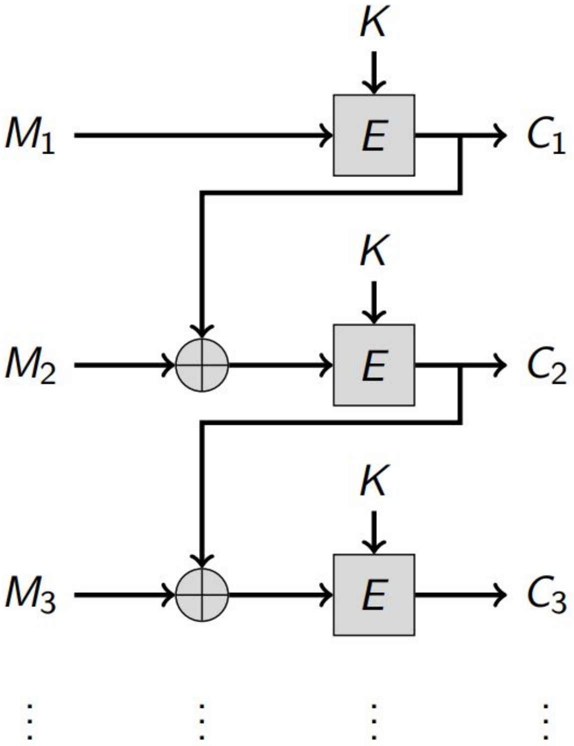
Q: Spot the difference?

Q: Is it fixed this time?

Q: Does this avoid repeating patterns among blocks?

Q: What would happen if we encrypt the message twice with the same key?

Attempt 2: ECB_2!!!



Q: Spot the difference?

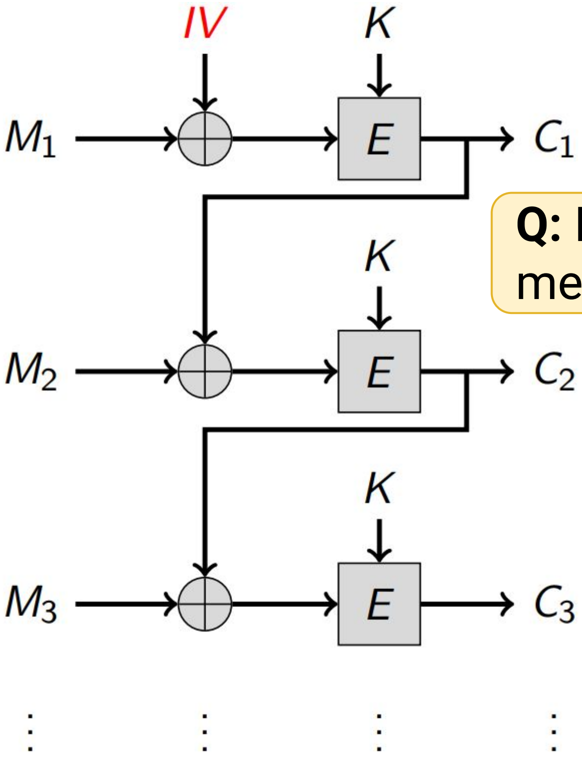
Q: Is it fixed this time?

Q: Does this avoid repeating patterns among blocks?

Q: What would happen if we encrypt the message twice with the same key?

A: $C_1 = E_K(M), C_2 = E_K(M) \Rightarrow C_1 = C_2$

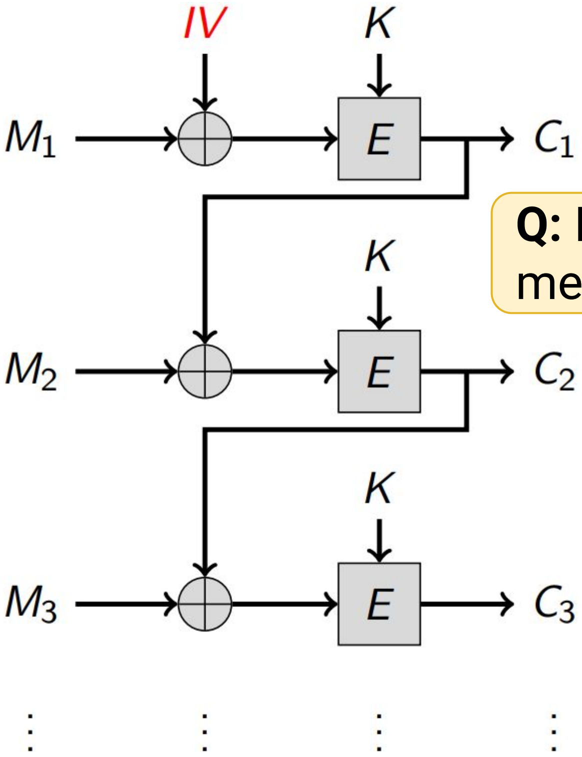
New Plan: CBC Mode



Q: Does this solve the issue of encrypting equal blocks?

Q: Does this solve the issue of encrypting equal messages/plaintexts?

New Plan: CBC Mode

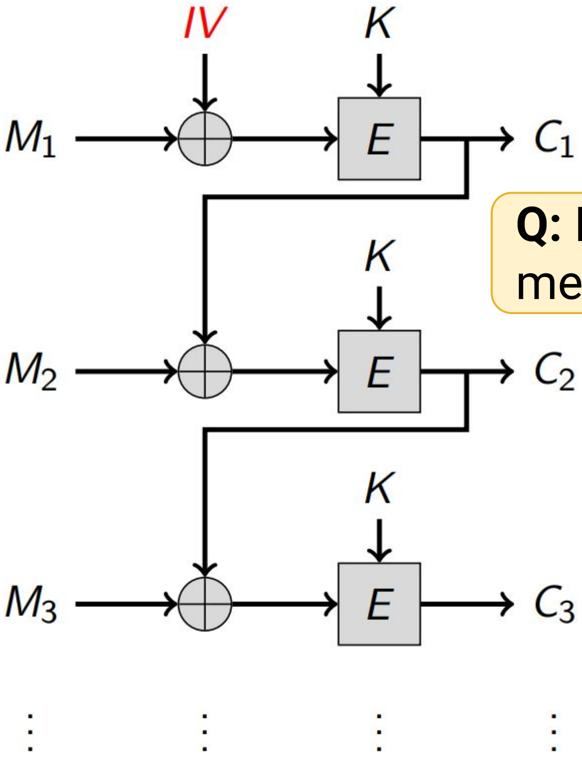


Q: Does this solve the issue of encrypting equal blocks?

Q: Does this solve the issue of encrypting equal messages/plaintexts?

A: Yes!!!

New Plan: CBC Mode



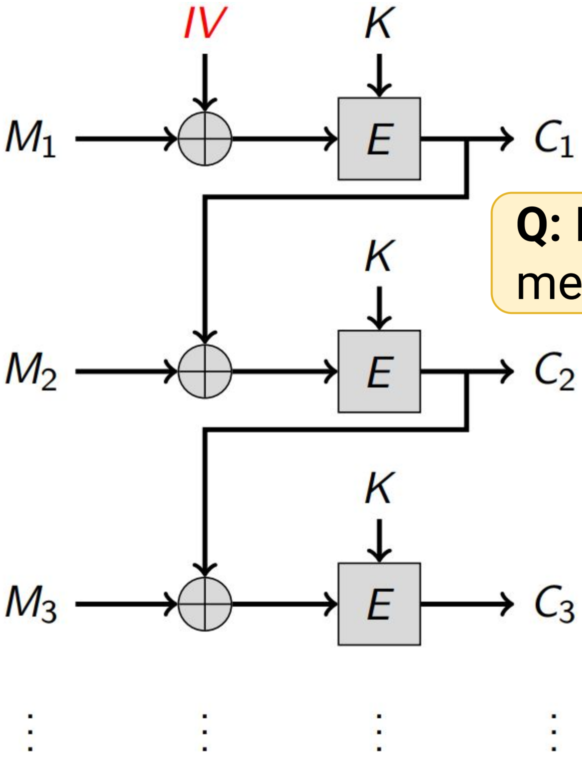
Q: Does this solve the issue of encrypting equal blocks?

Q: Does this solve the issue of encrypting equal messages/plaintexts?

A: Yes!!!

Q: Can we share IV in the clear?

New Plan: CBC Mode



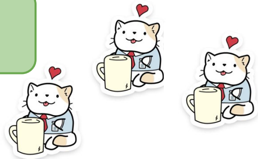
Q: Does this solve the issue of encrypting equal blocks?

Q: Does this solve the issue of encrypting equal messages/plaintexts?

A: Yes!!!

Q: Can we share IV in the clear?

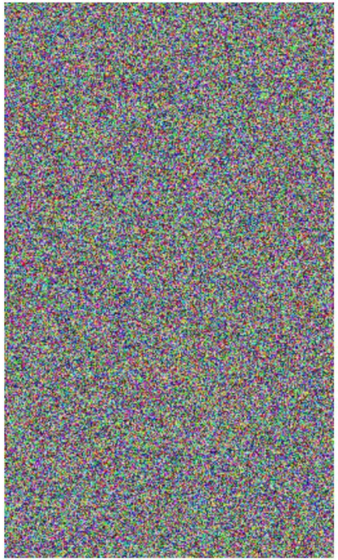
A: Yes!!!



IV, an initialization vector, nonce, salt.

Modes of Operation Collection

- Cipher Block Chaining **(CBC)**, Counter **(CTR)**, and Galois Counter **(GCM)** modes
- Patterns in the plaintext are no longer exposed because these modes involve some kind of "feedback" among different blocks.
- But you need an **IV**



So…now what?

- How do Alice and Bob share the secret key?
  - Meet in person; diplomatic courier…
- In general this is very hard

Or, we invent new technology!!

Spoiler Alert: it's already been invented…

Tuesdayyyyyyyyyy

Until next time...