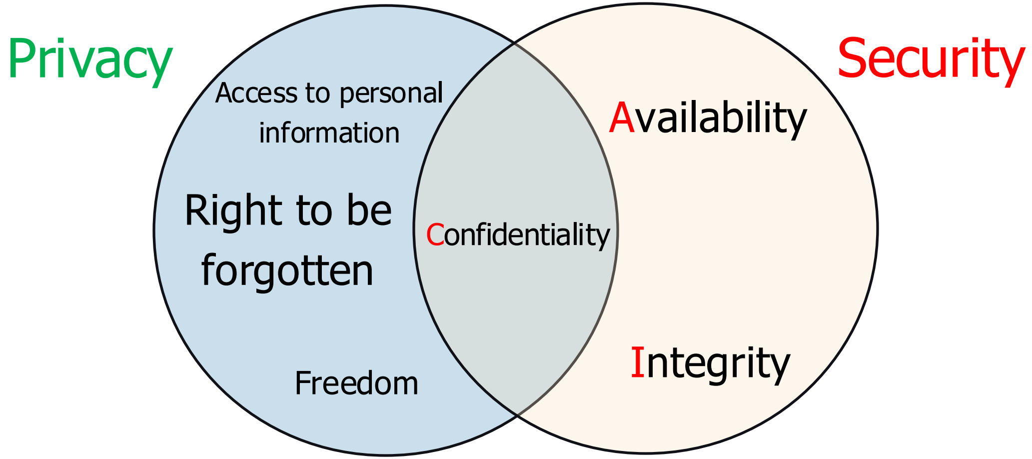
CS459/698 Privacy, Cryptography, Network and Data Security

Basics of Cryptography

Fall 2024, Tuesday/Thursday 02:30pm-03:50pm

Quick recap

- Security and Privacy? (rights vs responsibilities)
  - Explored how can we distinguish between privacy & security
  - Defined, **what** is being protected, from **who**, and under what **conditions** this protection will hold.
  - Gave a loose definition of assets, vulnerabilities, threats and attacks.

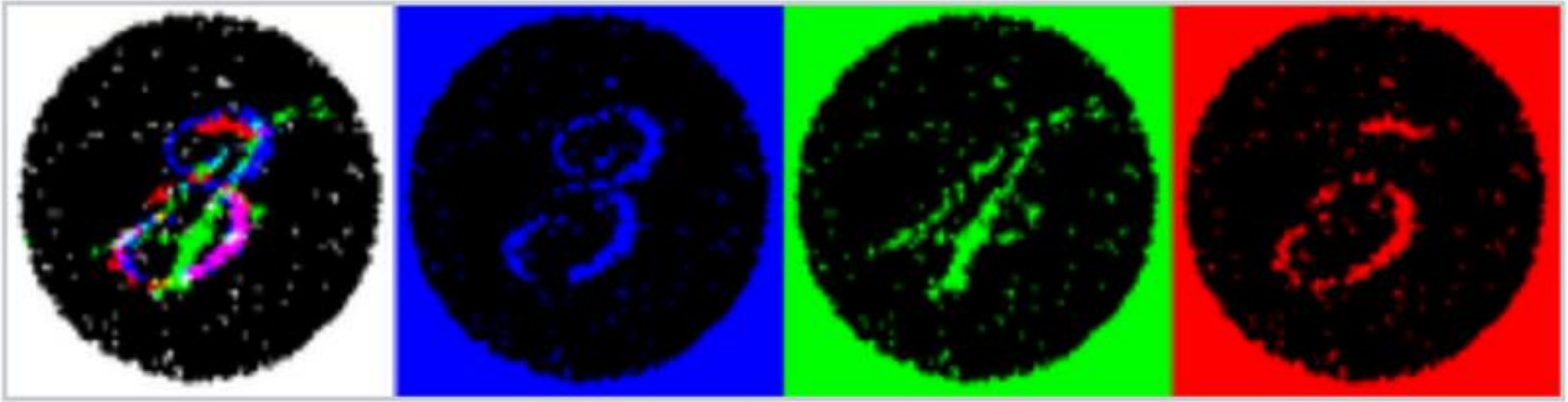


This lecture

- Identify attack techniques and apply them (Cryptanalysis)
  - Cryptanalysis: studies cryptographic systems to look for weaknesses or information leakage
- Explain building blocks of cryptography
  - Cryptography: Show how to send secure messages over an insecure medium (eg. Internet)
- Explain how modern cryptography properties arose

Goal: Why does Basically, know what cryptography tools exist and how to securely use them. Build a foundation of primitives 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 – Cast of characters

(Honest) communicating parties

Alice Bob Carol Dave

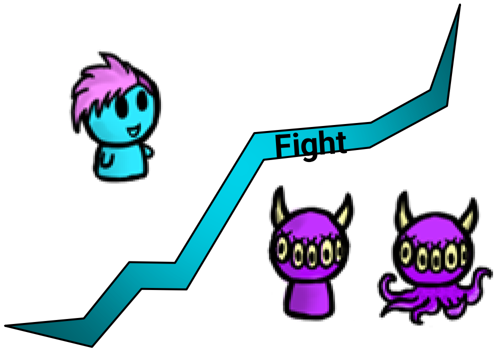
Adversaries

Eve Mallory

- Eve: a passive eavesdropper who can listen to transmitted messages
- Mallory: an active Man-In-The-Middle, who can listen to, and modify, insert, or delete, transmitted messages.

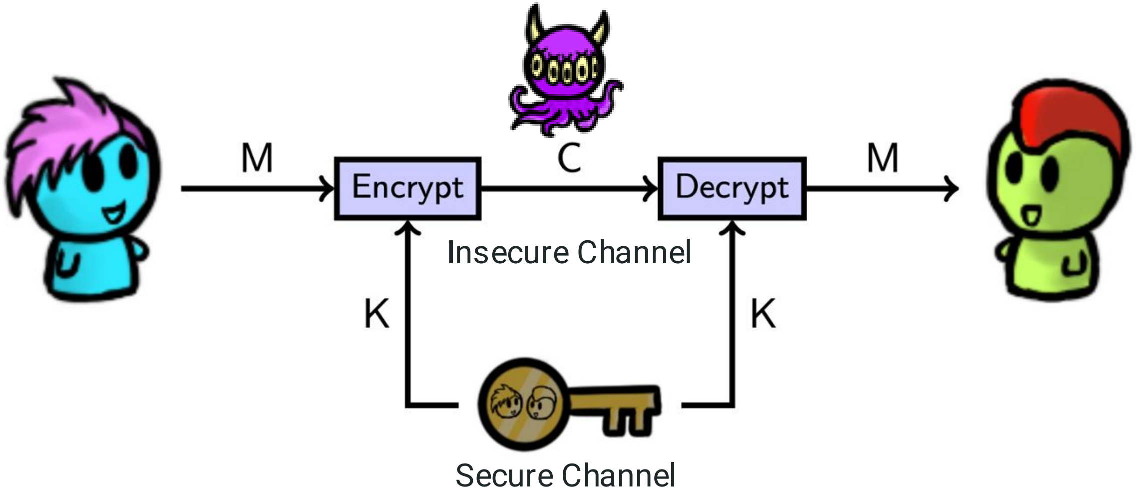
Components of Cryptography

- **C**onfidentiality
  - Preventing Eve from reading Alice's messages
- **I**ntegrity
  - Preventing Mallory from Modifying Alice's messages without being detected
- **A**uthenticity,
  - Preventing Mallory from impersonating Alice



Cryptography - Path for Secret Messages

- Secret-key encryption (symmetric encryption) is the simplest form of cryptography.
- The key Alice uses to encrypt the message is the same as the key Bob uses to decrypt it
- Eve, not knowing the key, should not be able to recover the plaintext



Historical Ciphers: Example One

FUBSWRJUDSKB

CRYPTOGRAPHY

Historical Ciphers: Example One

FUBSWRJUDSKB

CRYPTOGRAPHY

Substitution Cipher (shift 3):

Caesar Cipher

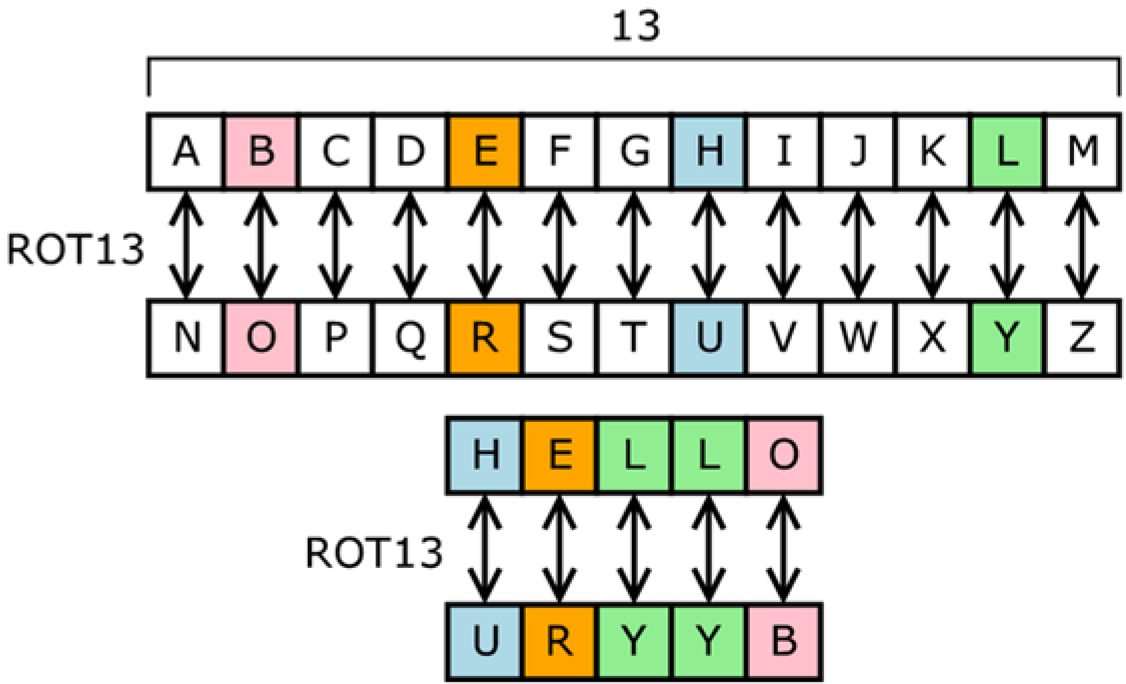


Image source: wikipedia

Caesar Cipher

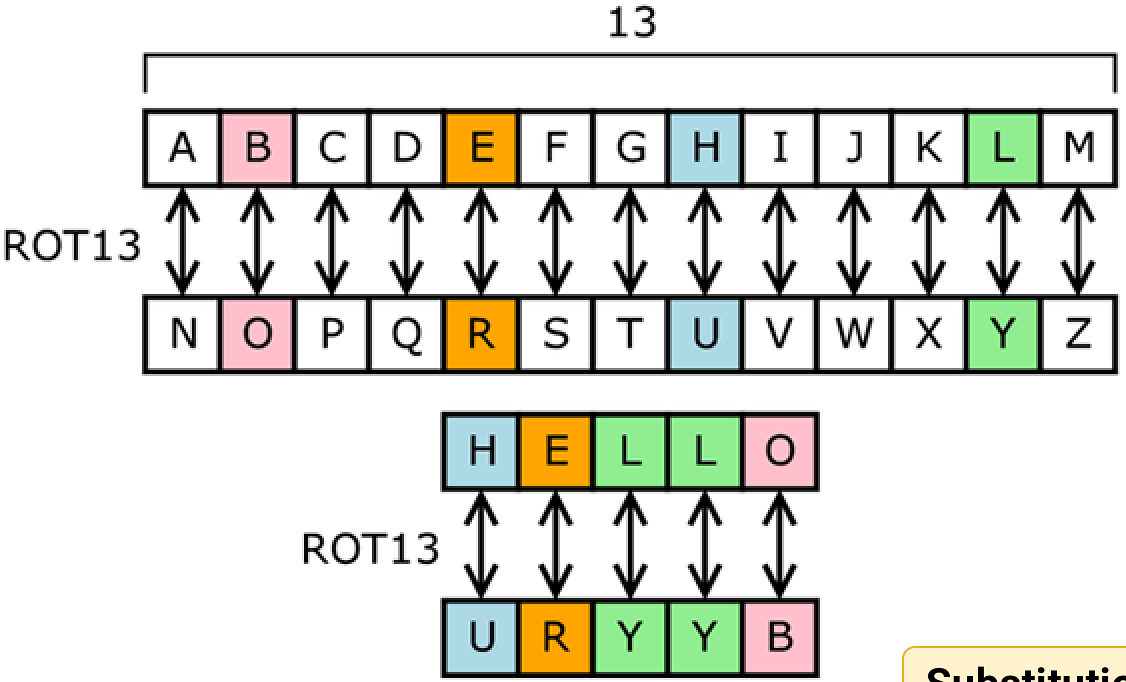


Image source: wikipedia

Substitution Cipher (shift 13)

Shift and Substitution Ciphers

Replace symbols (letters) by others

- Using a rule e.g., y = x + 13 (mod 26), Caesar‘s cipher Key: 13
- Using a keyword e.g, Key: table(t=a shift of 20.)

Cryptanalysis - Analyzing “secret” messages

Mwahaha

We will learn the secretsssss.

Historical Ciphers: Example Two

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

Historical Ciphers: Example Three – Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

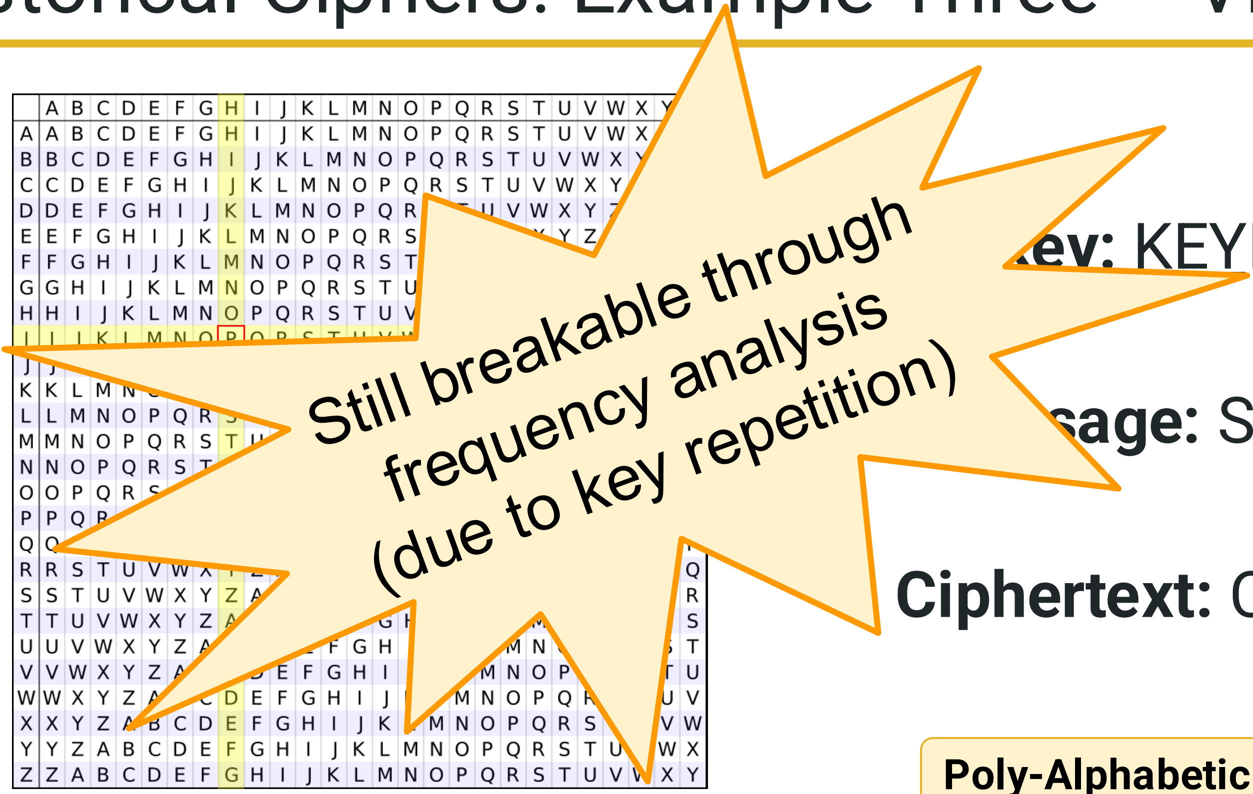
Key: KEYKEYKE

Message: SECURITY

Ciphertext: CIAEVGDC

Poly-Alphabetic Substitution Cipher

Historical Ciphers: Example Three – Vigenère



ey: KEYKEYKE

sage: SECURITY

Ciphertext: CIAEVGDC

Poly-Alphabetic Substitution Cipher

Historical Ciphers: Example Four

LECTURE SECURITY AND CRYPTOGRAPHY II

↓

LENGECDRCUCATRRRPUIYHRTPYEYTISAOI

Historical Ciphers: Example Four

LECTURES

ECURITYA

NDCRYPTO

GRAPHYII

→ **LENG**ECDRCUCATRRPUIYHRTPYEYTISAOI

Transposition Cipher

Historical Ciphers: Example Four

LECTURES

ECURITYA

NDCRYP

YHRTPYEYTISAOI

GRA

Shannon's maxim!!!! (design assuming adversaries will learn the algorithm)

Transposition Cipher

Kerckhoff’s Principle

- **Kerckhoff’s principle**: a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge.
  - The system is at most as secure as the number of keys(shortcuts to finding the key)

Kerckhoff’s Principle

- **Shannon’s maxim**: we should design systems under the assumption that the enemy will immediately gain full familiarity with them.
  - Don’t use “secret” encryption methods (security by obscurity)
  - Have public algorithms that use a secret key as input (easier to change the key than the whole system)

Vernam Cipher

- **Encrypts one bit at a time by XOR'ing the plaintext with the key:**
  - Plaintext (t bits): $M = [m_1, m_2, \ldots, m_t]$
  - Key (t bits): $K = [k_1, k_2, \ldots, k_t]$
  - Ciphertext (t bits): $C = [c_1, c_2, \ldots, c_t] = [m_1, m_2, \ldots, m_t] \oplus [k_1, k_2, \ldots, k_t]$
  - XOR reminder:

$0 \oplus 0 = 0$ $\quad$ $0 \oplus 1 = 1$ $\quad$ $1 \oplus 0 = 1$ $\quad$ $1 \oplus 1 = 0$

Q: How do we decrypt ?

A: $[m_1, m_2, \ldots, m_t] = [c_1, c_2, \ldots, c_t] \oplus [k_1, k_2, \ldots, k_t]$

- If K is randomly chosen and never reused, Vernam cipher is called One-Time Pad

One-time Pad

- Vernam cipher: C = M ⊕ K
- If K is randomly chosen and never reused, Vernam cipher is called One-Time Pad
    - This provides Information-Theoretic security (The key must be truly random≠PRG).

Q: Why does “trying every key” not work here ?

A: Because, given a ciphertext C, for every possible message M, there exist a key K that could have generated that ciphertext.

Two-time Pad?

Q: What happens if we use the same key K (therefor, same keystream) ?

$\text{Ciphertext}_1 = \text{Message}_1 \oplus K = \text{2c1549100043130b1000290a1b}$

$\text{Ciphertext}_2 = \text{Message}_2 \oplus K = \text{3f16421617175203114c020b1c}$

Hmmm… how can I relate these messages together?

Two-time Pad?

A: We can XOR the ciphertexts: $C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_1 \oplus K) = M_1 \oplus M_2$

$\text{Ciphertext}_1 \oplus \text{Ciphertext}_2 =$

$\text{Message}_1 \oplus K \oplus \text{Message}_2 \oplus K =$

$\text{Message}_1 \oplus \text{Message}_2 =$ 13030b06175441080 14c2b0107

Two-time Pad?

$\text{Message}_1 \oplus \text{Message}_2$ = 13030b0617544108014c2b0107

Suppose Message_1 starts with “Alice” (416C696365)

- Message_2 seems to start with readable text (“Rober”)

Two-time Pad?

$Message_1 \oplus Message_2$ = 13030b0617544108014c2b0107

Suppose It starts with “Alice and Bob” (416C6963652061 6E6420426F62)

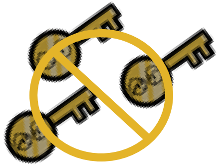
- $Message_2$ is fully readable now (“Rober feline”)

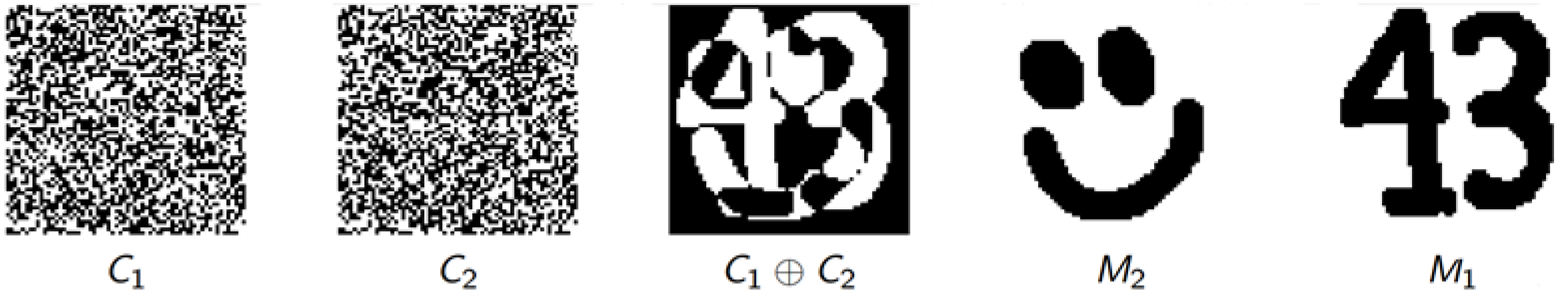
Ahaaa!

Two-time Pad?

Messages are not purely random!

- A “two-time pad” is insecure!
- The key must never be used more than once
- The key must be as long as the message





So…Cryptography?

- Simple substitution/transposition is insecure
- One-Time Pad is inefficient over the secure channel
  - Keys as long as messages – think about encrypting GBs of data!

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

Now what?

Substitution is insecure…

Transposition is insecure…

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

BUT…

Repeat it often enough and it can be regarded as secure

Now what?

Substitution is insecure…

Transposition is in…

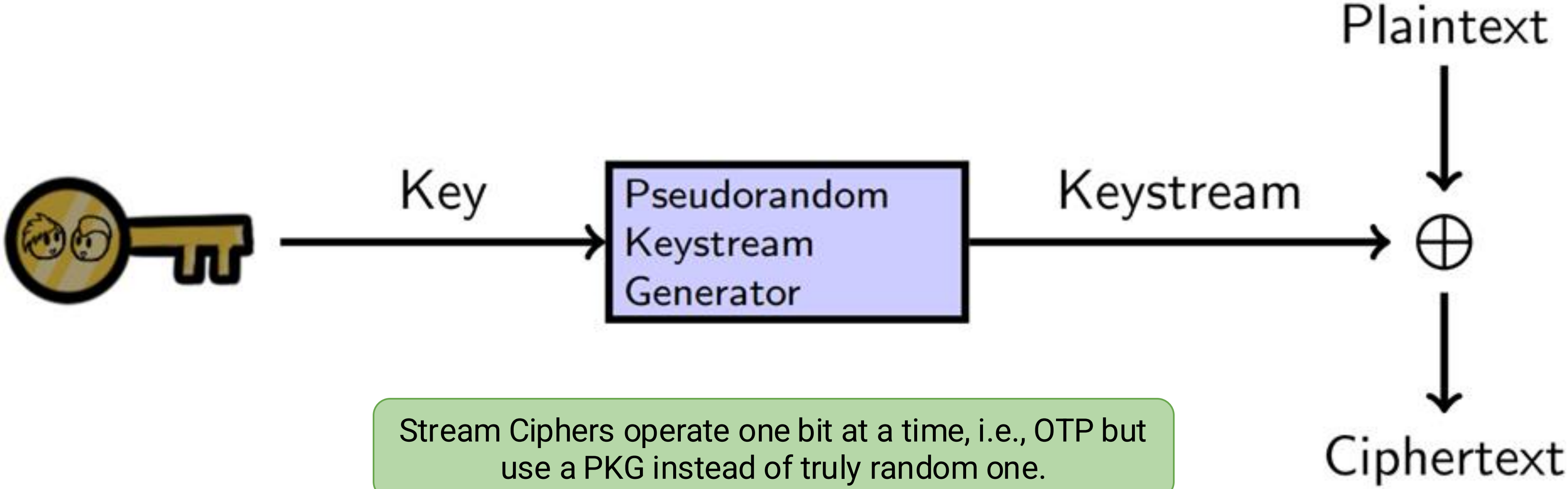
Key reuse … d) is insecure…

Stream Ciphers and Block Ciphers

BUT…

Rep… it often enough and it can be regarded as secure

Stream Cipher?



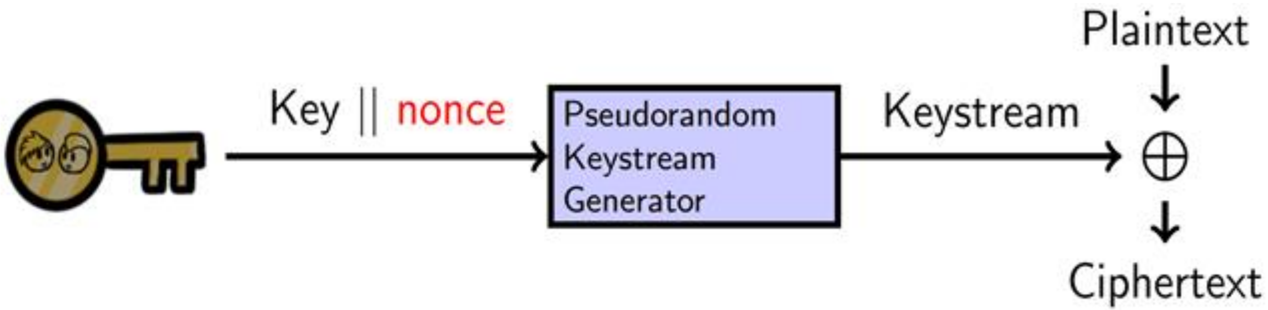
Stream Ciphers operate one bit at a time, i.e., OTP but use a PKG instead of truly random one.

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 (which does not need to be a secret)



Fun(?) Facts:

- WEP, PPTP are great examples of how not to use stream ciphers. "Susceptible to dictionary attacks and brute-force attacks"

Bit by bit…. but do you have to?

- Weakness of streams…one bit at a time?
  - What happens in a stream cipher if you change just one bit of the plaintext?

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

- Weakness of streams…one bit at a time?
  - What happens in a stream cipher if you change just one bit of the plaintext?

A: You only change a bit in the ciphertext

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

- Weakness of streams...one bit at a time?
  - What happens in a stream cipher if you change just one bit of the plaintext?

A: You only change a bit in the ciphertext

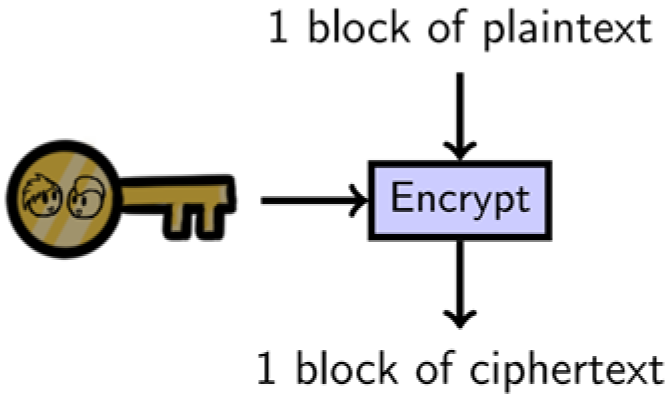
Q: Can we do better?

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

- Weakness of streams...one bit at a time?
  - What happens in a stream cipher if you change just one bit of the plaintext?

A: You only change a bit in the ciphertext

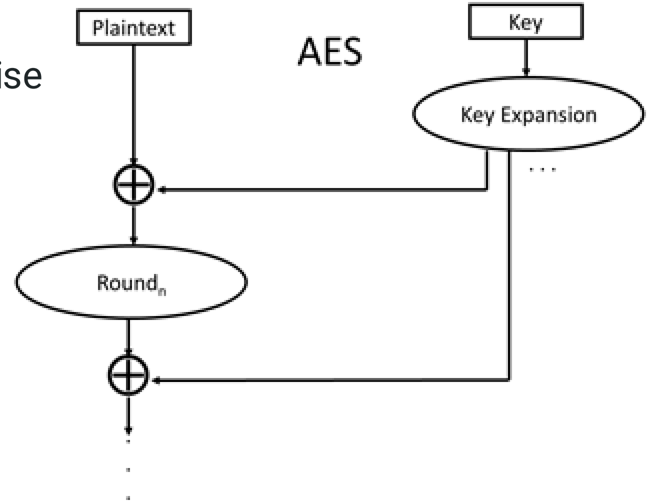
Q: Can we do better?



Block Ciphers !!!

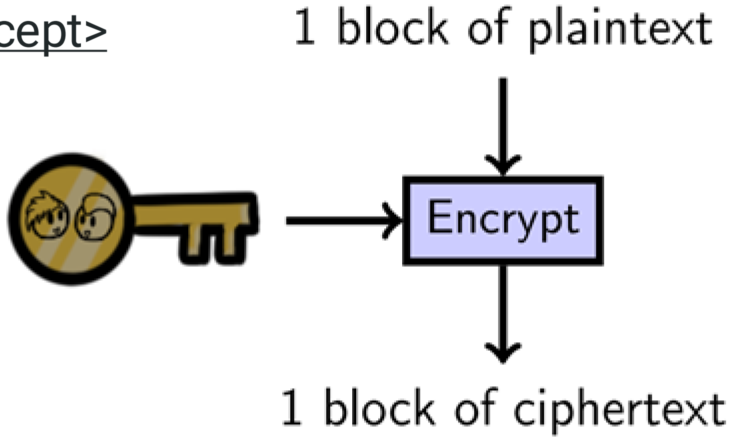
Block Ciphers

- 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

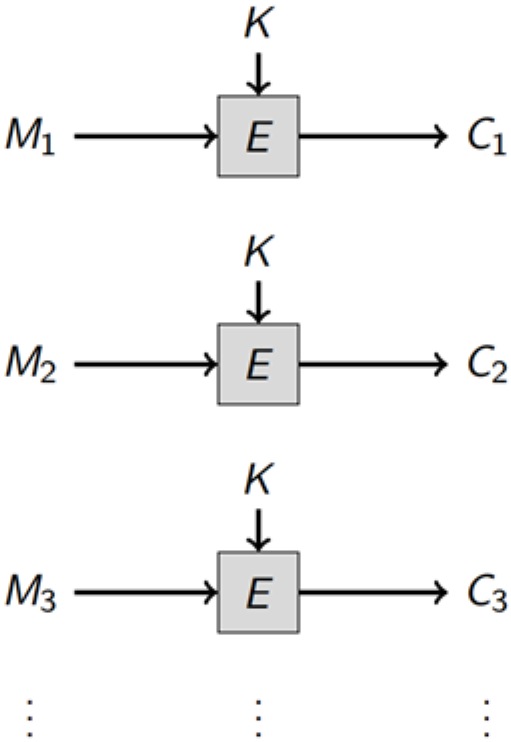


Two Catches with Block Ciphers

- Message is **shorter** than one block?
  - Requires padding
- Message is **longer** than a block?
  - Requires modes of operation <new concept>



Electronic Code Book (ECB) mode

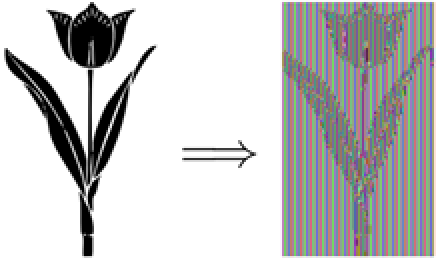


- Encrypts each successive block separately

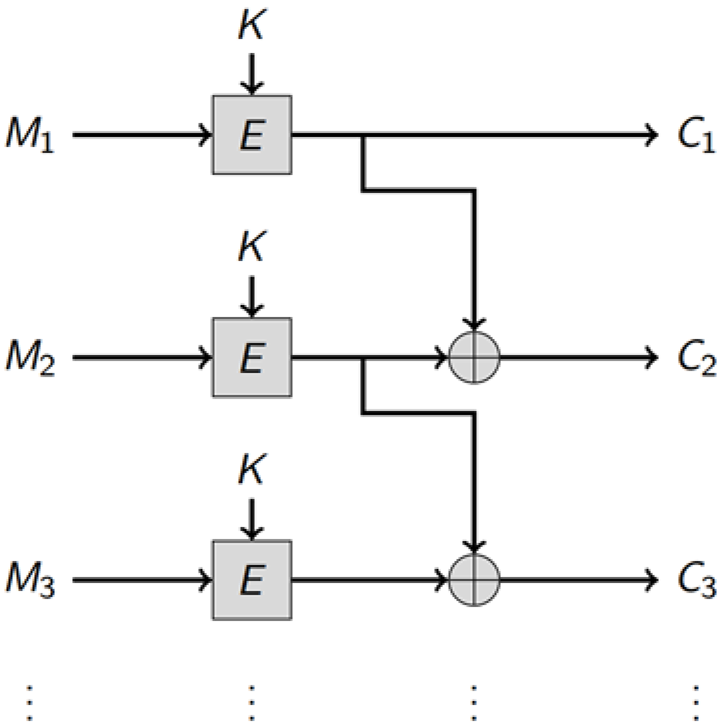
Q: What happens if the plaintext M has some blocks that are identical, $M_i = M_j$?

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

This reveals the pattern in the ciphertext…



Improving ECB (V_1)

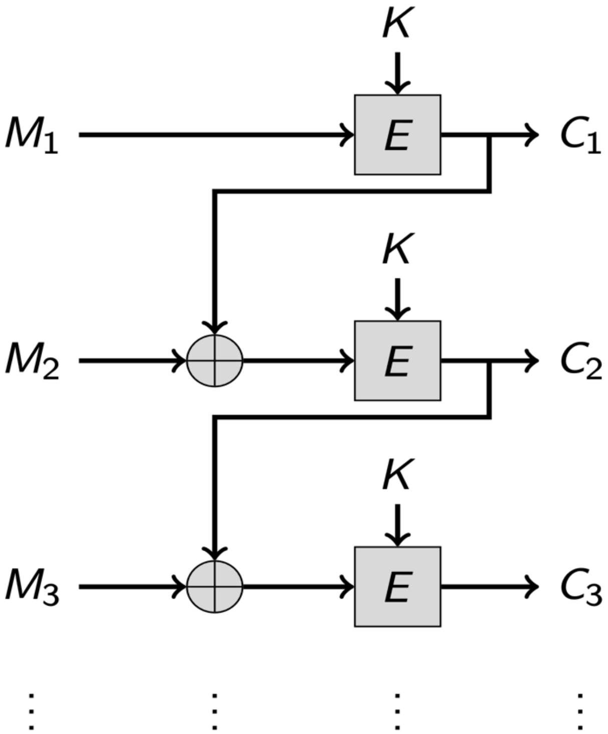


- We can provide “feedback” among different blocks, to avoid repeating patterns

Q: Does this avoid repeating patterns?
Are there other issues?

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

Improving ECB (V_2)



Q: Spot the difference?

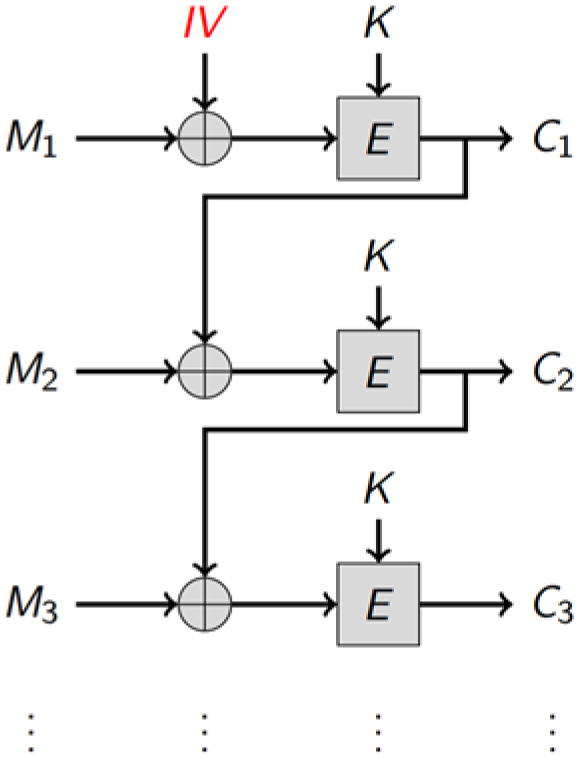
Q: Does this avoid repeating patterns among blocks?

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

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

We could change the key… but there is a better way

Cipher Block Chaining (CBC) mode

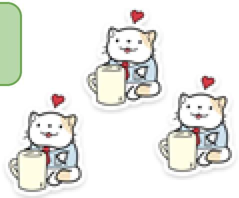


Q: Does this solve the issue of encrypting equal blocks? Does this solve the issue of encrypting equal messages/plaintexts?

A: Yes! CBC mode

Q: Can we share IV in the clear?

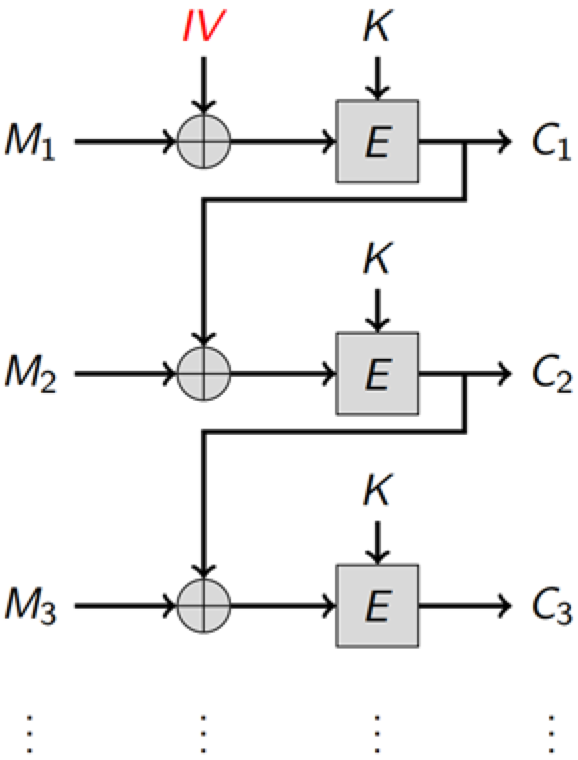
A: Yes!!!



An Initialization Vector might also be called as a nonce (number used once) or salt.

CBC Recap:

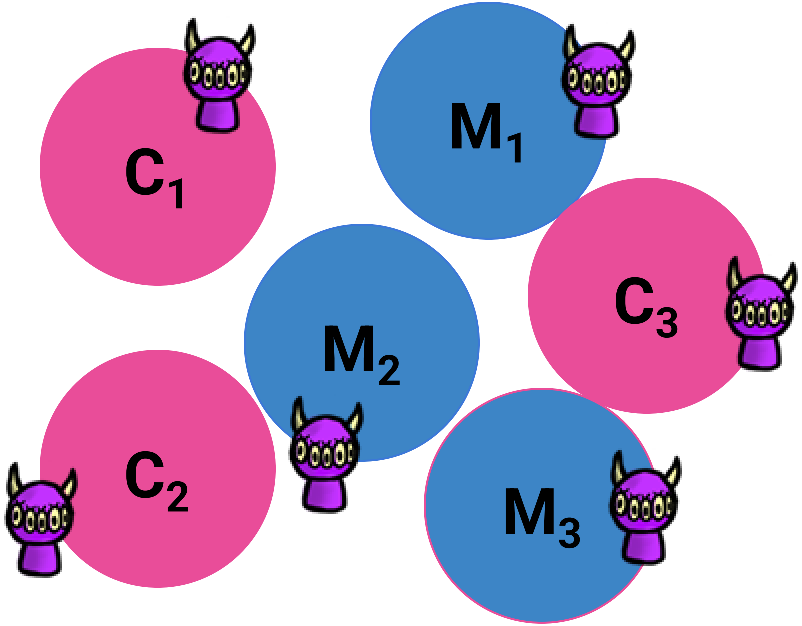
1. Generate a secret key K
2. Encrypt M using K and a generated IV
3. Decrypt C using K and the IV to get M



Security Goal: Indistinguishability under adaptive chosen ciphertext attack (IND-CCA2)

Cipher Security, IND-CCA2

Indistinguishability under Adaptive Chosen Ciphertext Attack

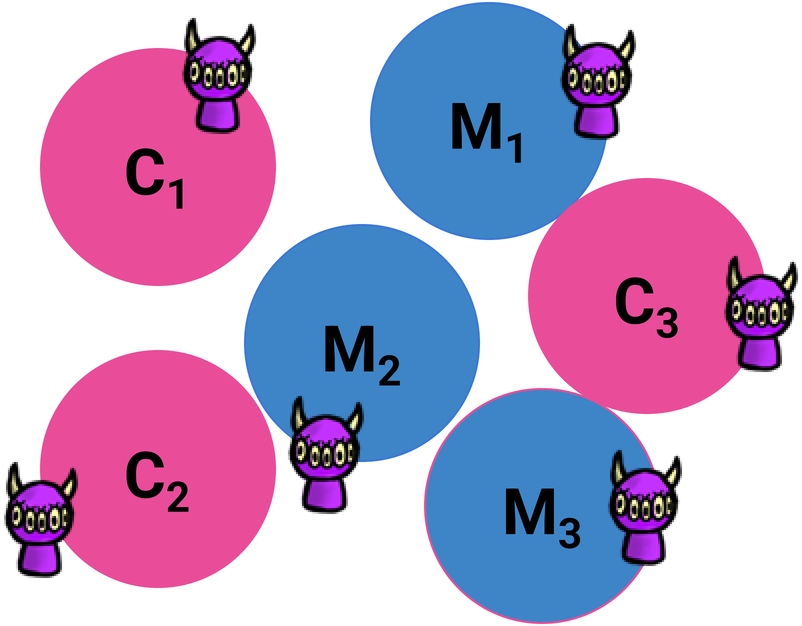


Adaptive chosen ciphertext attack

Eve exploits the ability to interact with the decryption oracle.

Cipher Security, IND-CCA2

Indistinguishability under Adaptive Chosen Ciphertext Attack



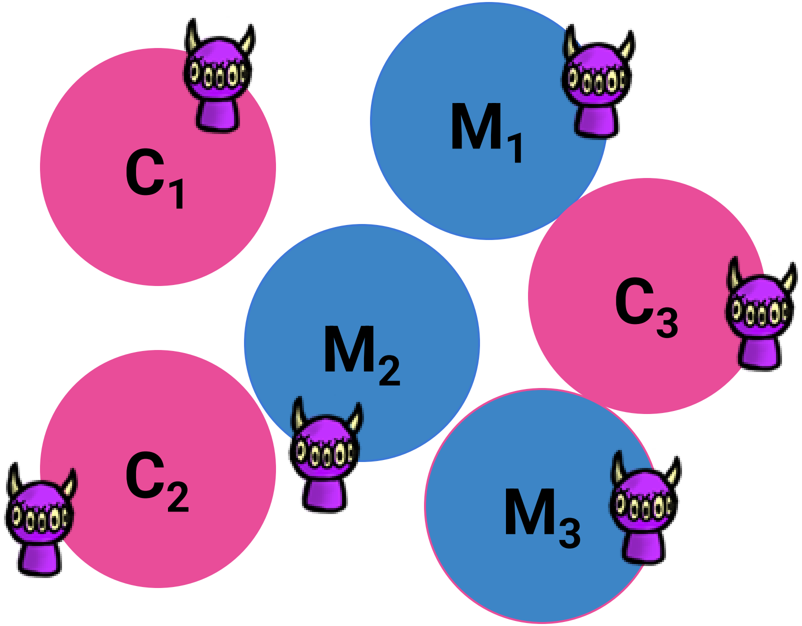
Adaptive chosen ciphertext attack

ACCA: Eve exploits the ability to interact with the decryption oracle.

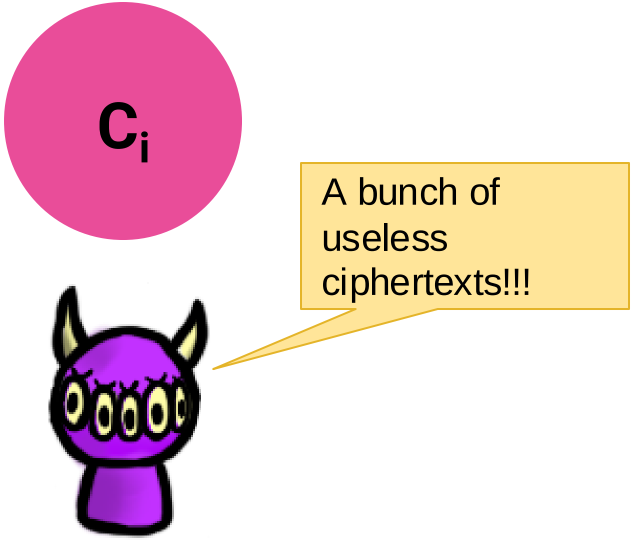
IND-CCA: Even if Eve can choose ciphertexts to be decrypted and has access to the decrypted results, they cannot distinguish between two different plaintexts based on their ciphertexts

Cipher Security, IND-CCA2

Indistinguishability under Adaptive Chosen Ciphertext Attack



Adaptive chosen ciphertext attack

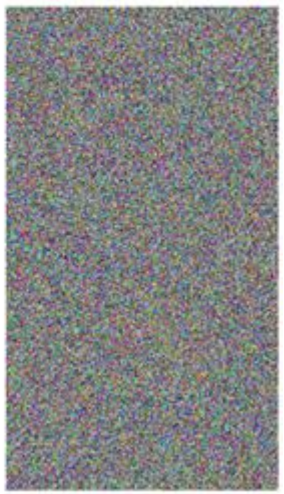


Eve cannot distinguish whether C_i is from M_1 , M_2 or M_3

Common modes of operation

- There are different modes of operation
    - e.g., 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 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…

Stay tuned!

Until next time…