

10/14/26

COMP 435:



Computer Security Concepts

Lecture 22: Cryptanalysis Cont. && One-Time Pad



The University
of North Carolina
at Chapel Hill

<https://tinyurl.com/comp435-fa26>

Logistics Update



- Lab 2 due today!
- Details about final project posted
 - First milestone due 10/21
- WA4 Next Friday. Crypto in Practice
 - Part 1 due 10/22
 - Part 2 in-class

Plan for Class Today

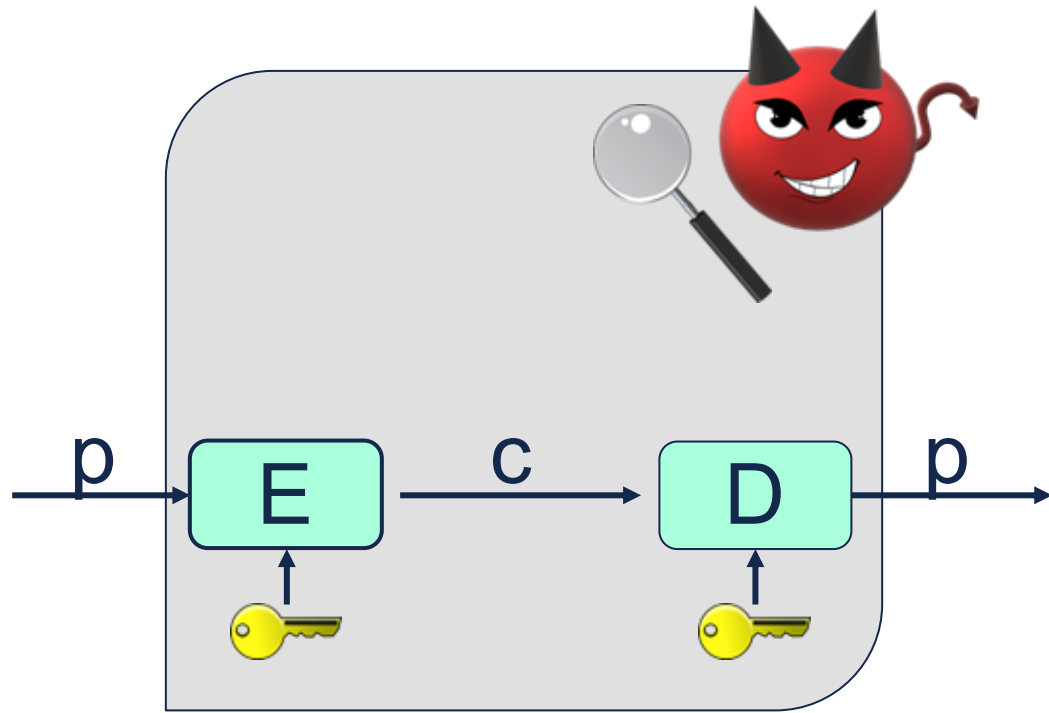


- 10:10-10:35 – Cryptanalysis
- 10:35- 11:00 – One Time Pad (OTP)

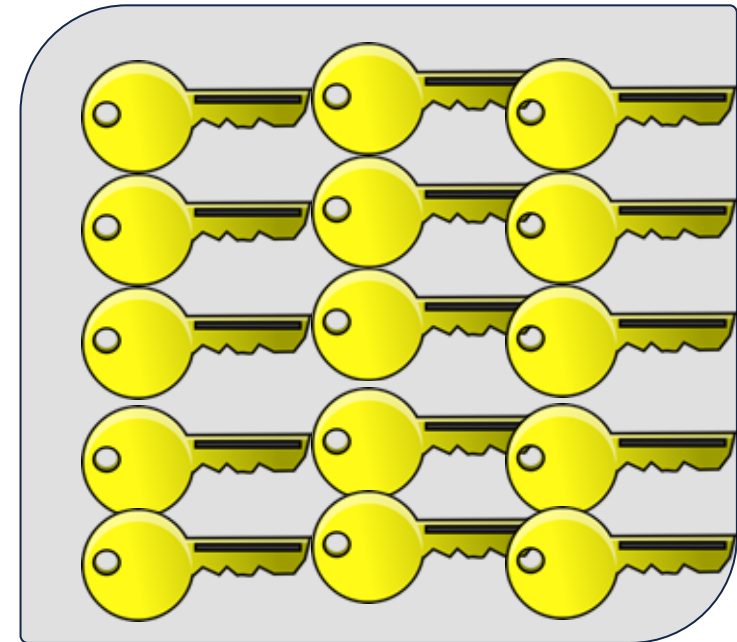
Guiding Question 😊

What does encryption
hide && what does it
still reveal??

Breaking Encryption



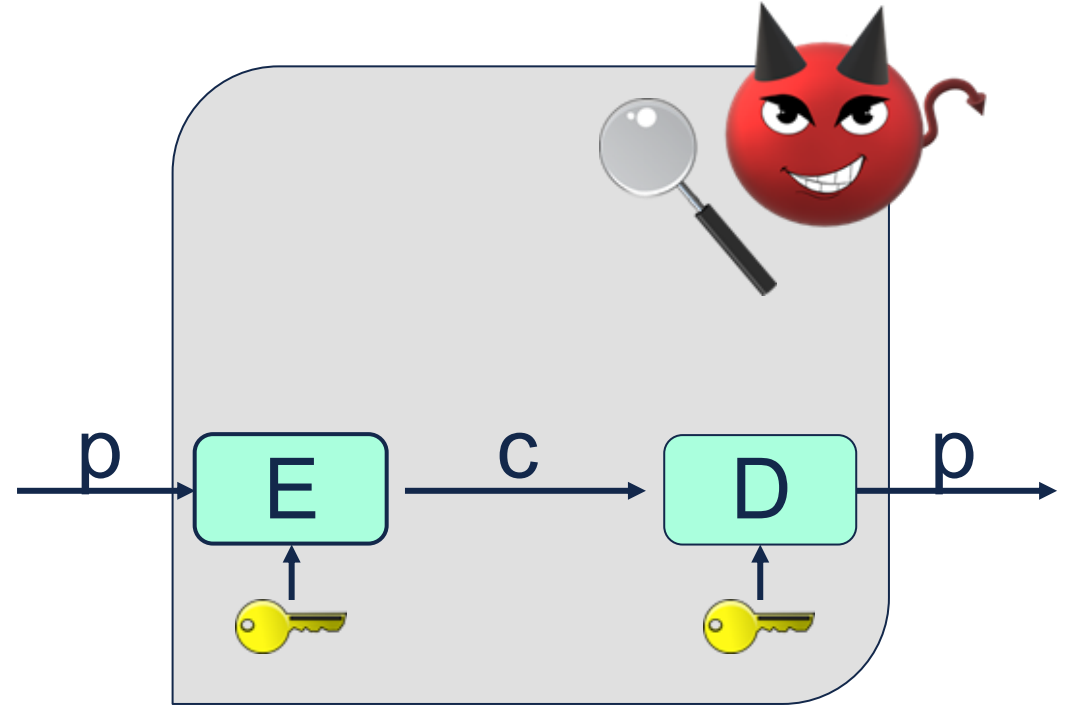
Cryptanalysis



Exhaustive
Search



Cryptanalysis



Cryptanalysis



Def'n: recover key material or plaintext by exploiting flaws in the cryptosystem

not necessarily whole key
or whole pt

Mono-Alphabetic Substitution



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



x e u a d n b k v m r o c q f s y h w g l z i j p t

26, 25, 24 ... → 26!

Mono-Alphabetic Substitution



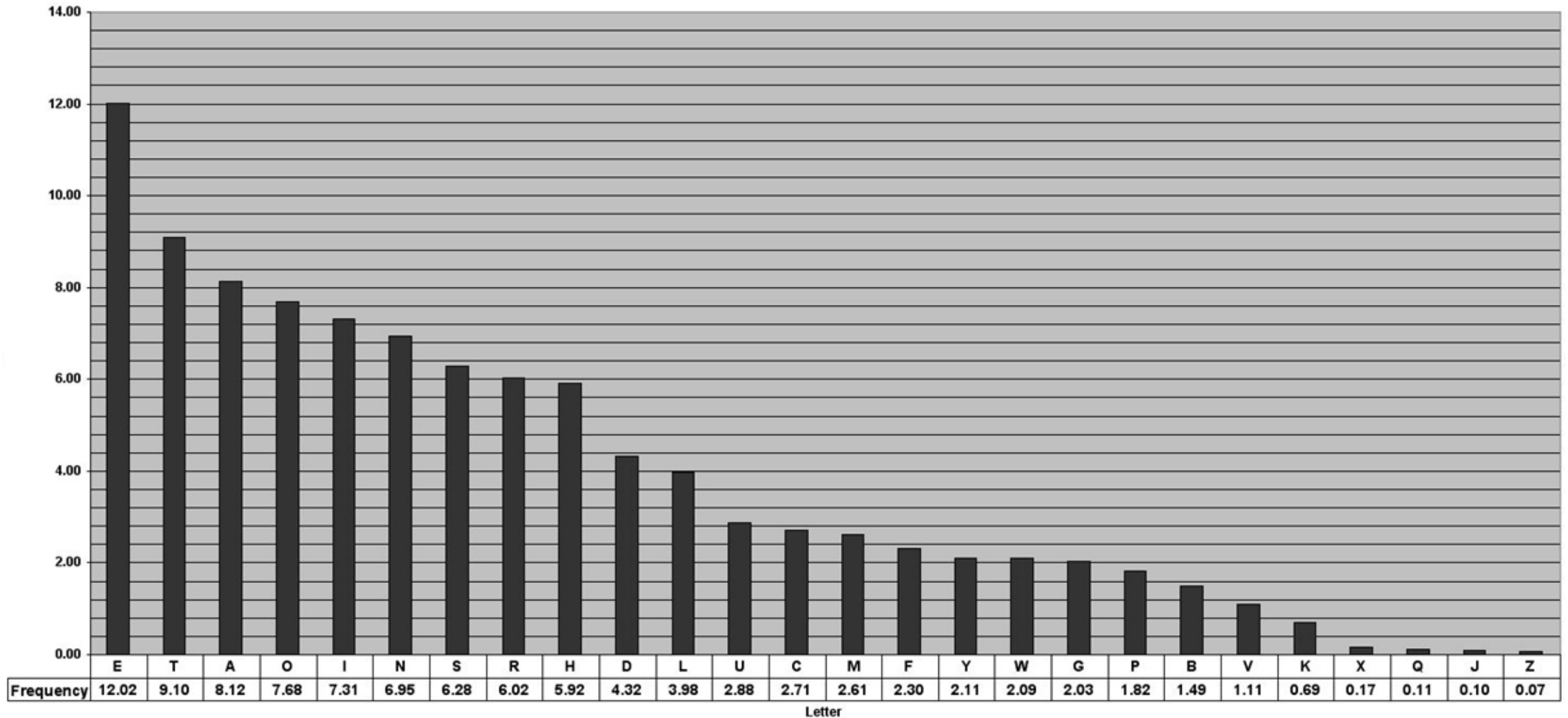
Number of keys to try: $26! \approx 2^{88}$

E.g.,

GDOOGKDCXEFLGCD

oo $\Rightarrow$ ~~ee~~, oo, TT,
FF, LL, ~~JJ~~

Letter Frequencies in English



Poly-Alphabetic Shift (Vigenère Cipher)



Plaintext:	^{0 1 2 3} tell them about me
Key:	cafe cafe cafec af
Ciphertext:	veqp vhjq cbtyv mj

$$\text{Enc}_k(m_i) \triangleq (m_i + k_i) \bmod 26$$

Cryptanalysis



- Cipher-text only attack
- Known-plaintext attack
- Chosen-plaintext attack (CPA)
- Chosen-ciphertext attack (CCA)

Cryptanalysis



- ***Cipher-text only attack***
- Known-plaintext attack
- Chosen-plaintext attack (CPA)
- Chosen-ciphertext attack (CCA)



adversary observes
ciphertexts

Cipher-text Only Attack

→ Set-up:
Enc, Dec, M = $\{0, 1\}^n$ 
K = $\{0, 1\}^p$



msg $\in$ M, key $\in$ K
ct = Enc_{key}(msg)

Given:

Enc, Dec, M, and a
ciphertext (ct)

Goal:

Recover a msg such that
m = Dec_{key}(ct)

Cipher-text Only Attack

Set-up:

Enc, Dec, $M = \{0, 1\}^n$ 

$K = \{0, 1\}^p$

$\text{msg} \in M, \text{key} \in K$

$\text{ct} = \text{Enc}_{\text{key}}(\text{msg})$



Given:

Enc, Dec, M , and a ciphertext (ct)

Goal:

Recover a msg such that
 $m = \text{Dec}_{\text{key}}(\text{ct})$

Enc = Mono-alphabetic substitution

$M = \{\text{"banana", "orange"}\}$

ct = xmqmqm

→

Attacker can figure out $m = \text{"banana"}$

Example

Cryptanalysis



- Cipher-text only attack
- ***Known-plaintext attack*** ←
- Chosen-plaintext attack (CPA)
- Chosen-ciphertext attack (CCA)

(m, C_t)

adversary learns
plaintext-ciphertext
pairs

Known-Plaintext Attack

Given:

Enc, Dec, M,
(m_1, c_1), (m_2, c_2) ... (m_j, c_j)
and a ciphertext (ct_i)

Goal:

Recover the msg such that
 $m_i = \text{Dec}_{\text{key}}(ct_i)$

Set-up:

Enc, Dec, $M = \{0, 1\}^n$ 

$K = \{0, 1\}^p$

$m_1, m_2 \dots m_j \in M, \text{key} \in K$

$ct_1 = \text{Enc}_{\text{key}}(m_1)$

$ct_2 = \text{Enc}_{\text{key}}(m_2) \dots$

$ct_j = \text{Enc}_{\text{key}}(m_j)$



Known-Plaintext Attack

Set-up:

Enc, Dec, $M = \{0, 1\}^n$ 

$K = \{0, 1\}^p$

$m_1, m_2 \dots m_j \in M, \text{key} \in K$

$\mathbf{ct}_1 = \mathbf{Enc}_{\text{key}}(m_1)$

$\mathbf{ct}_2 = \mathbf{Enc}_{\text{key}}(m_2) \dots$

$\mathbf{ct}_j = \mathbf{Enc}_{\text{key}}(m_j)$



Given:

Enc, Dec, M ,

$(m_1, c_1), (m_2, c_2) \dots (m_j, c_j)$

and a ciphertext (ct_i)

Goal:

Recover the msg such that

$\mathbf{m}_i = \mathbf{Dec}_{\text{key}}(\mathbf{ct}_i)$

Enc = Shift Cipher

Given $(m_1, c_1) = ("abc", "cfg")$



Attacker can recover the key and
decrypt any future message!

Example

Cryptanalysis



- Cipher-text only attack
- Known-plaintext attack
- ***Chosen-plaintext attack (CPA)***
- Chosen-ciphertext attack (CCA)



Adversary can
obtain ciphertext
for plaintext of its
choosing

Chosen-Plaintext Attack

Given:

Enc, Dec, M, **ct** and

$$\mathbf{ct}_1 = \mathbf{Enc}_{\text{key}}(m_1)$$

$$\mathbf{ct}_2 = \mathbf{Enc}_{\text{key}}(m_2) \dots$$

$$\mathbf{ct}_j = \mathbf{Enc}_{\text{key}}(m_j)$$

Goal:

Recover the msg such that

$$\mathbf{msg} = \mathbf{Dec}_{\text{key}}(\mathbf{ct})$$

Set-up:

Enc, Dec, $M = \{0, 1\}^n$ 

$$K = \{0, 1\}^p$$

$m \in M, \text{key} \in K$

$$\mathbf{ct} = \mathbf{Enc}_{\text{key}}(m)$$



To be CPA-Secure, a scheme must be
non-deterministic.

Determinism



- **Deterministic encryption:** the same plaintext encrypted with the same key always produces the same ciphertext.
- For CPA, that is dangerous because an attacker can encrypt chosen messages and compare outputs to recognize or infer future messages.

Chosen-Plaintext Attack

Given:

Enc, Dec, M, **ct** and

ct₁ = Enc_{key}(m₁)

ct₂ = Enc_{key}(m₂) ...

ct_j = Enc_{key}(m_j)

Goal:

Recover the msg such that

msg = Dec_{key}(**ct**)

Set-up:

Enc, Dec, M = {0, 1}ⁿ 

K = {0, 1}^p

m ∈ M, key ∈ K

ct = Enc_{key}(m)



K = {a-z}³

key: "key"

> M = {"a", "b", "c"}



CPA adversary can request
Enc("a"), Enc("b"), Enc("c"),
Enc("a") again, and learn the key

Example

Cryptanalysis



- Cipher-text only attack
- Known-plaintext attack
- Chosen-plaintext attack (CPA)
- ***Chosen-ciphertext attack (CCA)***



Adversary can
obtain decryption
for ciphertext of its
choosing

Chosen-Ciphertext Attack

Given:

Enc, Dec, M, **ct** and

$m_1 = \text{Dec}_{\text{key}}(\text{ct}_1)$

$m_2 = \text{Dec}_{\text{key}}(\text{ct}_2) \dots$

$m_j = \text{Dec}_{\text{key}}(\text{ct}_j)$

Goal:

Recover the msg such that

$\text{msg} = \text{Dec}_{\text{key}}(\text{ct})$

Set-up:

Enc, Dec, $M = \{0, 1\}^n$ 

$K = \{0, 1\}^p$

$m \in M, \text{key} \in K$

$\text{ct} = \text{Enc}_{\text{key}}(m)$



To be CCA-Secure, a scheme must be **non-malleable**.

Malleability



- Malleable: an attacker can modify a ciphertext in a predictable way that causes a related change in the decrypted plaintext.
- An encryption scheme is non-malleable if:
 - If the adversary modifies a given ciphertext, the result is either an illegal ciphertext or one that encrypts a plaintext having no relation to the original one
- E.g., if the attacker is trying to break the encrypted ciphertext c , the attacker is free to flip just the first bit of c and send that new ciphertext c' to the oracle to be decrypted.
 - Therefore, to be secure against CCA attacks, it must be the case that c' is either an illegal ciphertext or is the ciphertext of something totally unrelated to the message that produced c .

Chosen-Ciphertext Attack

Given:

Enc, Dec, M, **ct** and

$$m_1 = \text{Dec}_{\text{key}}(\text{ct}_1)$$

$$m_2 = \text{Dec}_{\text{key}}(\text{ct}_2) \dots$$

$$m_j = \text{Dec}_{\text{key}}(\text{ct}_j)$$

Goal:

Recover the msg such that

$$\text{msg} = \text{Dec}_{\text{key}}(\text{ct})$$

want to learn
m = Dec(ct)

Set-up:

Enc, Dec, $M = \{0, 1\}^n$ 

$$K = \{0, 1\}^p$$

$$m \in M, \text{key} \in K$$



$$\text{ct} = \text{Enc}_{\text{key}}(m)$$

$$K = \{0, 1\}^8$$

Want to decrypt some given ct



Chooses: $c_1 = \text{ct} \text{ XOR } 0000_0001$

Can query: $m_1 = \text{Dec}_k(c_1)$ to try to
recover m such that $m = \text{Dec}_k(\text{ct})$

Example

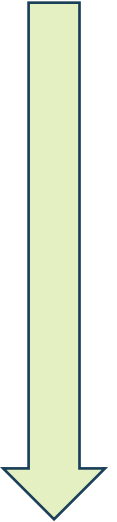
Cryptanalysis



- Cipher-text only attack
- Known-plaintext attack
- Chosen-plaintext attack (CPA)
- Chosen-ciphertext attack (CCA)

passive attacks

active attacks



Stronger

WS Q3 from last time!

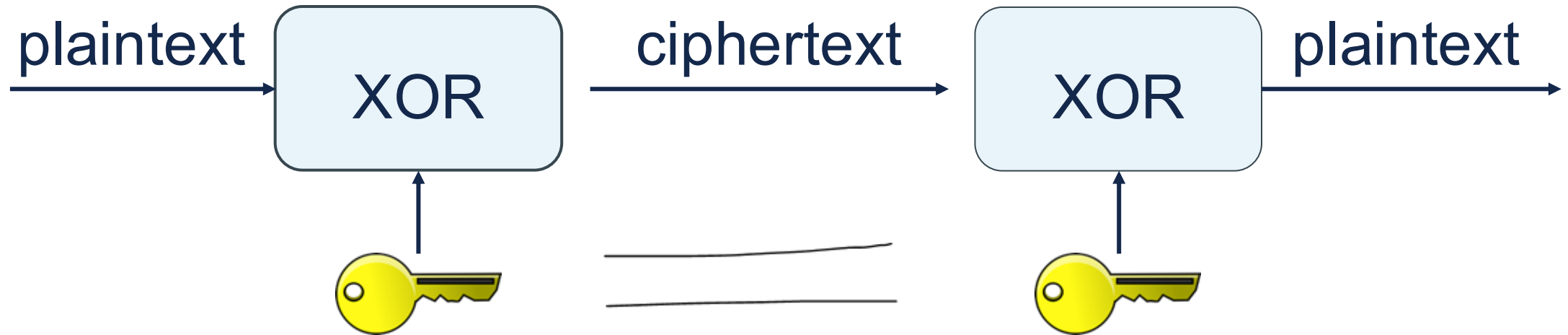


X perfect Security

One Time Pad

One Time Pad (Vernam Cipher)

Pt
 $K : \{0,1\}^n$
 Ct



$$c_i = p_i \oplus k_i$$

$$p_i = c_i \oplus k_i$$

$(mod 2)$

One Time Pad (Vernam Cipher): Encryption



plaintext		0	1	0	0	0	0	0	1
key	$\oplus$	0	1	0	1	0	1	0	1
ciphertext		0	0	0	1	0	1	0	0

One Time Pad (Vernam Cipher): Decryption



ciphertext		0	0	0	1	0	1	0	0
	$\oplus$								
key		0	1	0	1	0	1	0	1
plaintext		0	1	0	0	0	0	0	1

One Time Pad (Vernam Cipher)



- ***Symmetric encryption algorithm***
- Stream cipher
- Substitution cipher



single key used
for encryption and
decryption

One Time Pad (Vernam Cipher)



- Symmetric encryption algorithm
- ***Stream cipher***
- Substitution cipher



each unit of the
plaintext is
encrypted
individually using
the corresponding
unit of the key

One Time Pad (Vernam Cipher)



- Symmetric encryption algorithm
- Stream cipher
- ***Substitution cipher***



each unit of the
plaintext is
replaced with a
unit of ciphertext

One Time Pad Keys



- Key material is as long as message
- ~~•~~ Key material is never reused ★
- Key material is kept secret
- Key material is chosen uniformly at random



One Time Pad

- Key material is as long as message
- Key material is never reused
- Key material is kept secret
- Key material is chosen uniformly at random

OTP offers ***information-theoretical security***

A hand-drawn, dark grey wavy line that starts with a small peak, dips into a valley, and then rises back to a level slightly higher than the start.

Information-Theoretical Security



Def'n: Security derives from information theory

OTP is information-theoretically secure:

- Attacker cannot recover plaintext without the key
 - Not susceptible to cryptanalysis
 - Not susceptible to exhaustive search
-

CCA

Today's Worksheet 😊 -- Just the Front

OTP



~~X~~ Confidential

- Provides **perfect secrecy**
- Does not provide integrity
 - Even though attacker can't read msg, attacker can modify it in a predictable way
- Difficult to use in practice
 - Managing key distribution & key storage is hard!