CS405 – Computer Security

Lab01 – Classical Cryptography

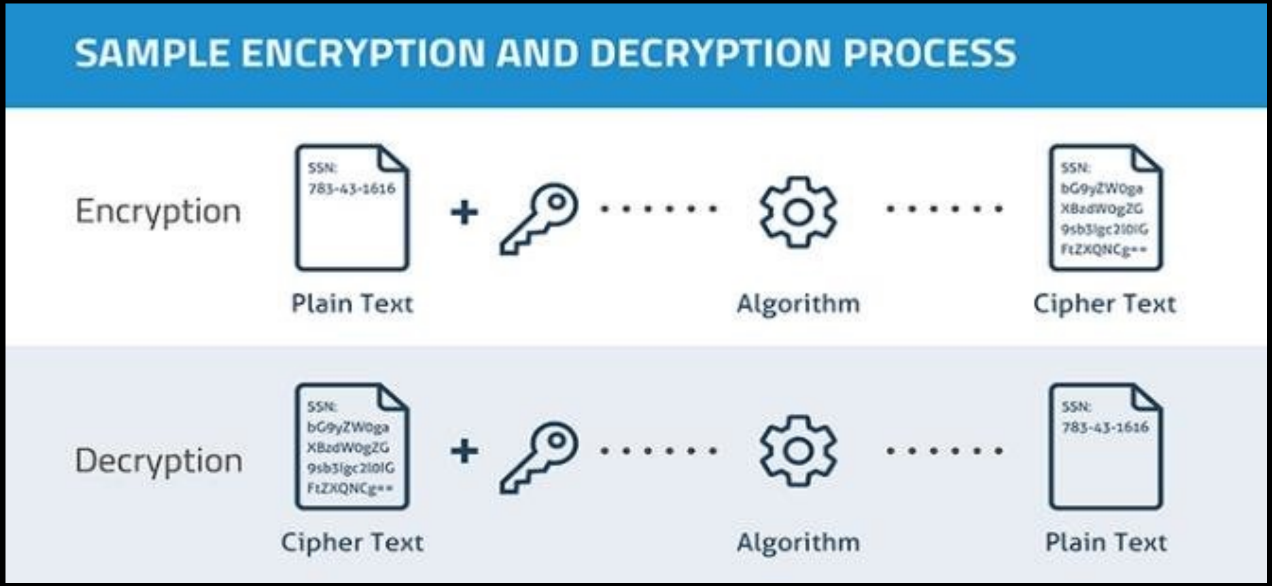
Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Introduction

- What is a ciphertext and a plaintext?
  - Ciphertext: data that is unreadable and looks like random data.
  - Plaintext: data that is readable and includes meaningful information.

Introduction

- Cryptosystems are a set of tools/algorithms that allows protecting our secret data by applying cryptographic algorithms.
- Cryptosystems have two important operations:
  - Encryption: transforming a plaintext into a ciphertext.
  - Decryption: recovering the ciphertext to a plaintext.



Introduction

- Cryptography is not just about encryption and decryption, it includes:
  - Hashing algorithms
  - Authentication algorithms
  - Key generation algorithms
  - Data communication protocols (TLS and secret key sharing)
  - Secure Multi-Party Computation (MPC)
  - Homomorphic encryption – a special type
  - Zero-knowledge proofs
- Data hiding techniques: steganography
- Obfuscation: securing code to protect against reverse engineering

Introduction

- Cryptography is used to maintain the following:
  - **Confidentiality**: Only authorized parties can read the protected information.
  - **Authentication**: You know that you are talking to the right entity/person and that they have not delegated their identity.
  - **Integrity**: A message hasn’t been changed between the sender and receiver.

Introduction

- A basic cipher takes bits and returns bits; it doesn’t care whether bits represents text, an image, or a PDF document.
- The ciphertext may in turn been coded as raw bytes, hexadecimal characters, base64, and other formats.
- What if you need the ciphertext to have the same format as the plain-text, as is sometimes required by database systems that can only record data in a prescribed format? Format Preserving Encryption

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Caeser Cipher

- One of the simplest and oldest methods of encrypting messages.
- It shifts the letters of the alphabet by a fixed number of places.
- Example, shift the letters by 1:

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

- HELLO WORLD encodes to IFMMP XPSME.

Caeser Cipher

- Shift by 2:

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

- The message HELLO WORLD is encoded as JGNNQ YQTNF

Caeser Cipher

- Implement Caeser cipher in python.

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Caeser Cipher

- Assume that you have this ciphertext encrypted with Caeser cipher, but the shift amount is unknown. Can you recover it?

“Px pbee fxxm hg Fhgwtr”

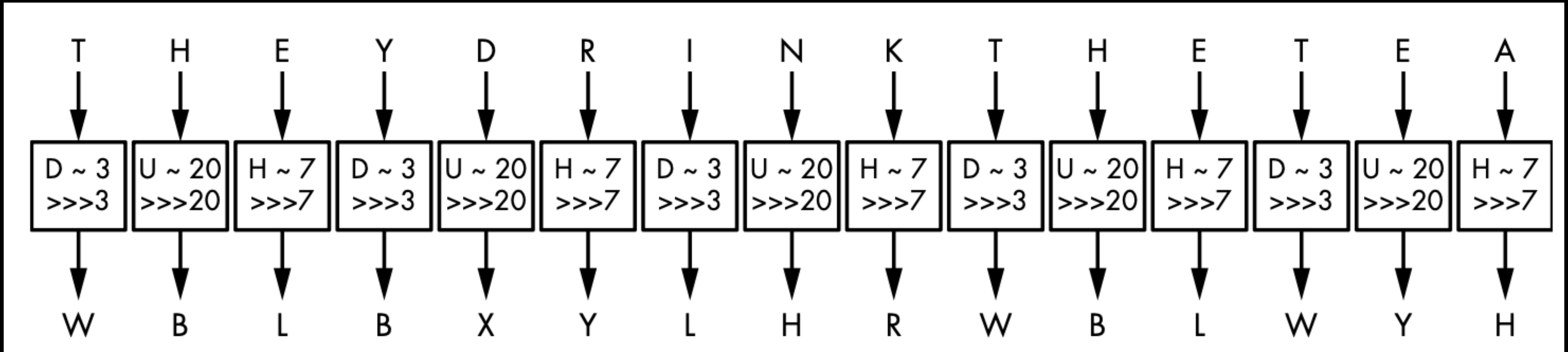
Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Vigenère Cipher

- Similar to the Caesar cipher, except that letters are shifted by values defined by a key.
  - The key is a collection of letters that represent numbers based on their position in the alphabet.
- For example, if the key is DUH, letters in the plaintext are shifted using the values D=3, U=20, H=7.
- The 3, 20, 7 pattern repeats until you’ve encrypted the entire plaintext.

Vigenère Cipher

- Example: encrypting the sentence THEY DRINK THE TEA using the keyword DUH



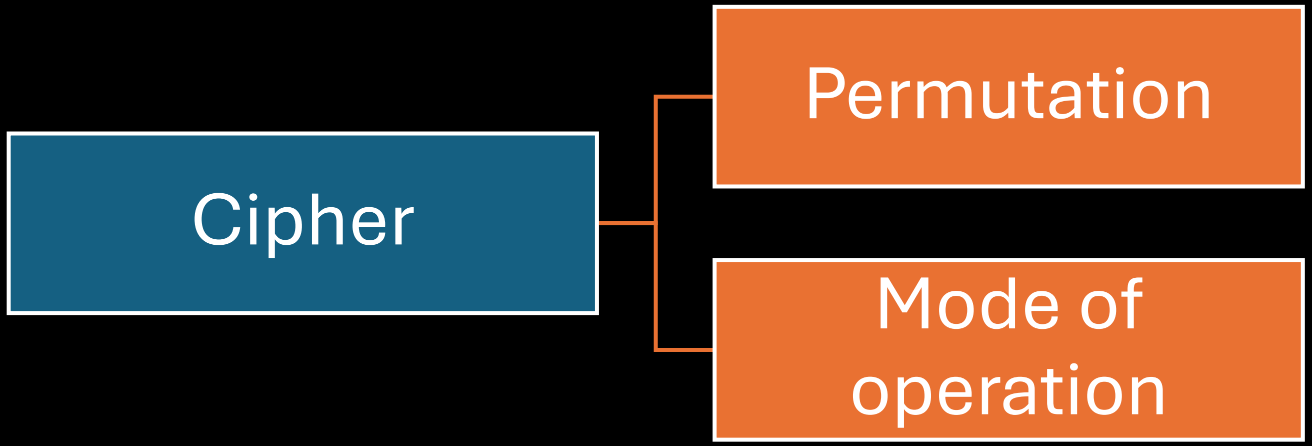
Vigenère Cipher

- Implement the Vigenère Cipher

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

How Ciphers Work?

- Each cipher has two components:

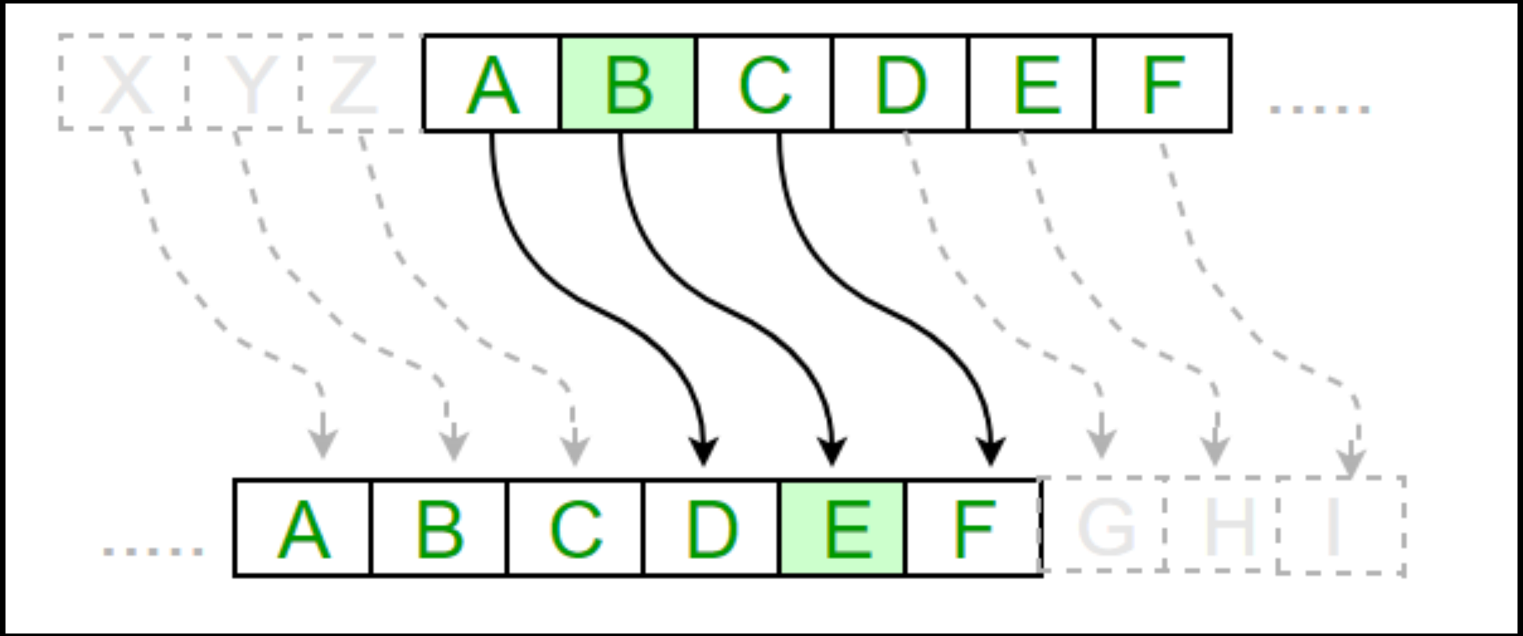


A function that transforms an item (a letter or a group of bits) such that each item has a unique inverse.

An algorithm that uses a permutation to process messages of arbitrary size.

How Ciphers Work?

- In Caeser cipher:
  - The permutation is just shifting the letters.
  - The mode of operation is repeating the same permutation, shifting, for each letter.



How Ciphers Work?

- Vigenère cipher has a more complex mode:
  - The permutation as Caeser cipher, just shifting each letter.
  - The mode of operation is different for each letter.

Plain Text	P	A	S	S	W	O	R	D
Key	K	E	Y	K	E	Y	K	E
Cipher Text	Z	E	Q	C	A	M	B	H

Content

The Permutation

- Most of the classical ciphers work by replacing each letter with another letter.
  - They are performing *substitution* – shifting in the alphabet.

- A “substitution” is different from a “permutation”.

- For example:
  - A function that transforms A, B, C, D to D, A, A, C is a “substitution”
  - A function that transforms A, B, C, D to C, A, D, B is a “permutation”
    - With a permutation, each letter has exactly one inverse.

The Permutation

- Not every permutation is secure. In order to be secure, a cipher's permutation should satisfy three criteria:

The permutation should be determined by the key.

Different keys should result in different permutations.

The permutation should look random.

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Mode of Operation

- Say we have a secure permutation that transforms A to X, B to M, and N to L.
  - Then, to encrypt BANANA, we get MXLXLX.

- Using the same permutation for all the letters in the plaintext thus reveals any duplicate letters in the plaintext.

- By analyzing these duplicates, you might not learn the entire message, but you'll learn something about the message.

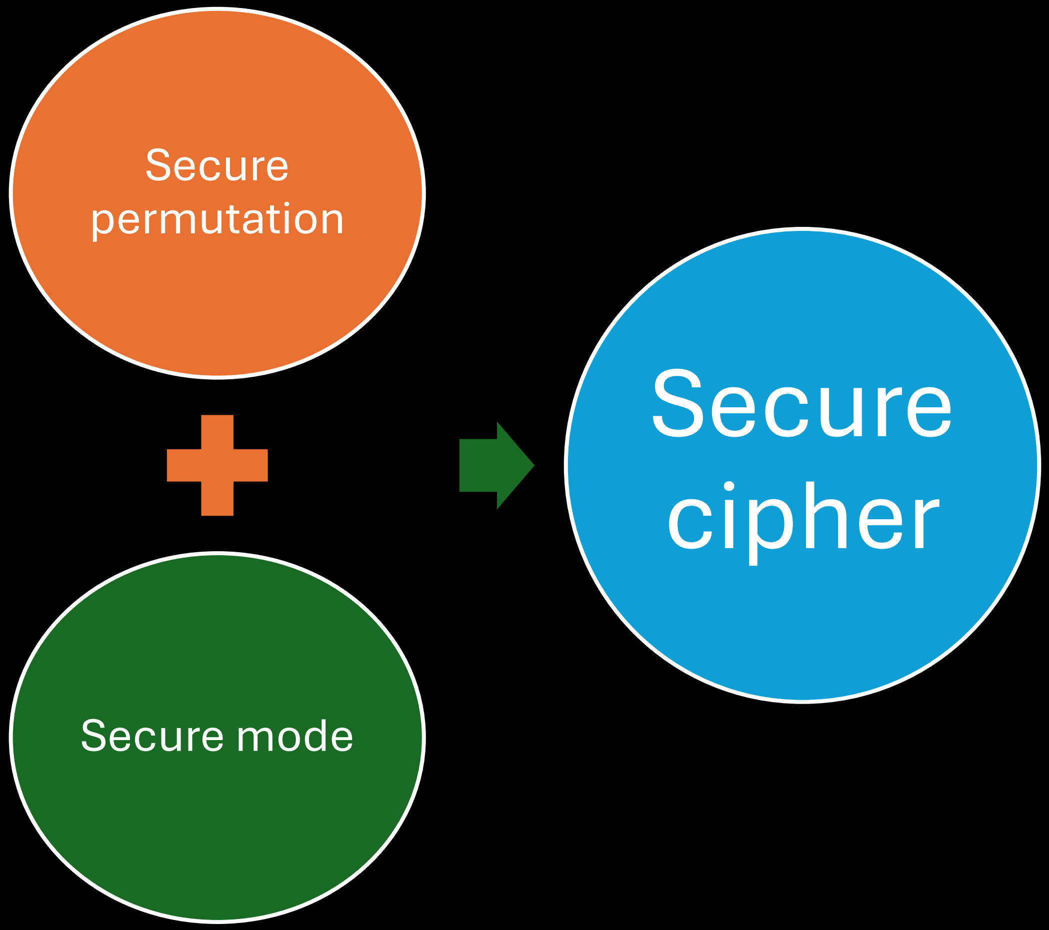
Mode of Operation

- The mode of a cipher mitigates the exposure of duplicate letters in the plaintext by using different permutations for duplicate letters.

- Vigenère cipher partially addresses this: if the key is N letters long, then N different permutations will be used for every N consecutive letters.
  - However, this can still result in patterns in the ciphertext because every Nth letter of the message uses the same permutation.

- Frequency analysis can be used to break Vigenère cipher.

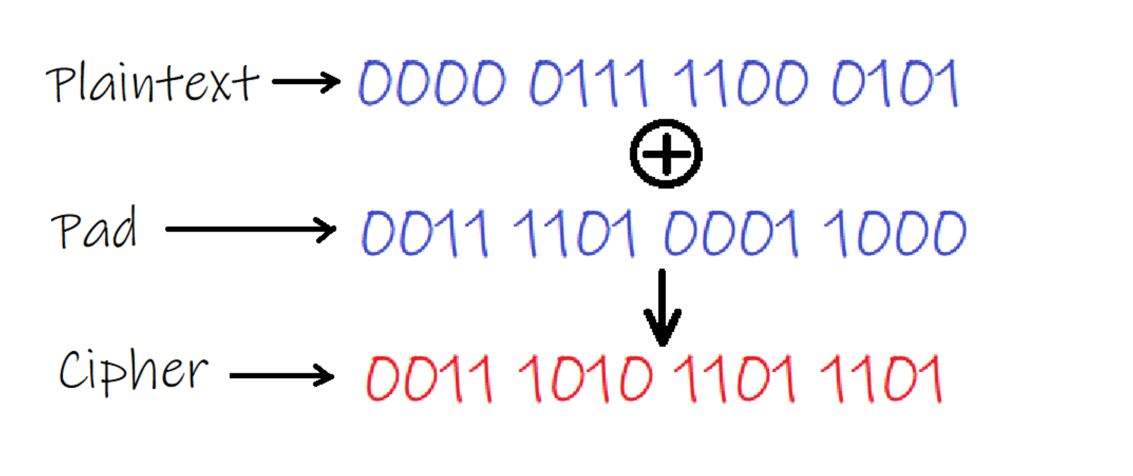
The Mode of Operation



Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

The One-Time Pad

- A cipher that cannot be cracked but requires the use of a **single-use** key that is larger than or equal to the size of the message being sent.



- perfect secrecy: if an attacker has unlimited computing power, it’s impossible to learn anything about the plaintext, but its length.

The One-Time Pad

Example: $P = 01101101$ and $K = 10110100$, then

- To encrypt: $C = P \oplus K = 01101101 \oplus 10110100 = 11011001$
- To decrypt: $P = C \oplus K = 11011001 \oplus 10110100 = 01101101$

	P	0	1	1	0	1	1	0	1
Encrypt: XOR	K	1	0	1	1	0	1	0	0
	C	1	1	0	1	1	0	0	1
Decrypt: XOR	K	1	0	1	1	0	1	0	0
	P	0	1	1	0	1	1	0	1

The One-Time Pad

- The important thing is that a one-time pad can only be used one time.
  - Each key K should be used only once.
  - If the same K is used to encrypt P1 and P2 to C1 and C2, then an eavesdropper can compute the following:

$$C_1 \oplus C_2 = (P_1 \oplus K) \oplus (P_2 \oplus K) = P_1 \oplus P_2$$

- Thus, an eavesdropper can learn the XOR difference of P1 and P2.
  - If either plaintext message is known, then the other message can be recovered.
- OTP is inconvenient: to encrypt a one-terabyte hard drive, you'd need another one-terabyte drive to store the key!

The One-Time Pad

- Implement the one-time pad.

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Encryption Security

- A cipher is secure if even given large number of plaintext and ciphertext pairs, nothing can be learned about the the cipher.

- Two concepts describe the security of a cipher:
  - Attack models: assumption about what an attacker can do.
  - Security goals: description of what is considered a successful attack.

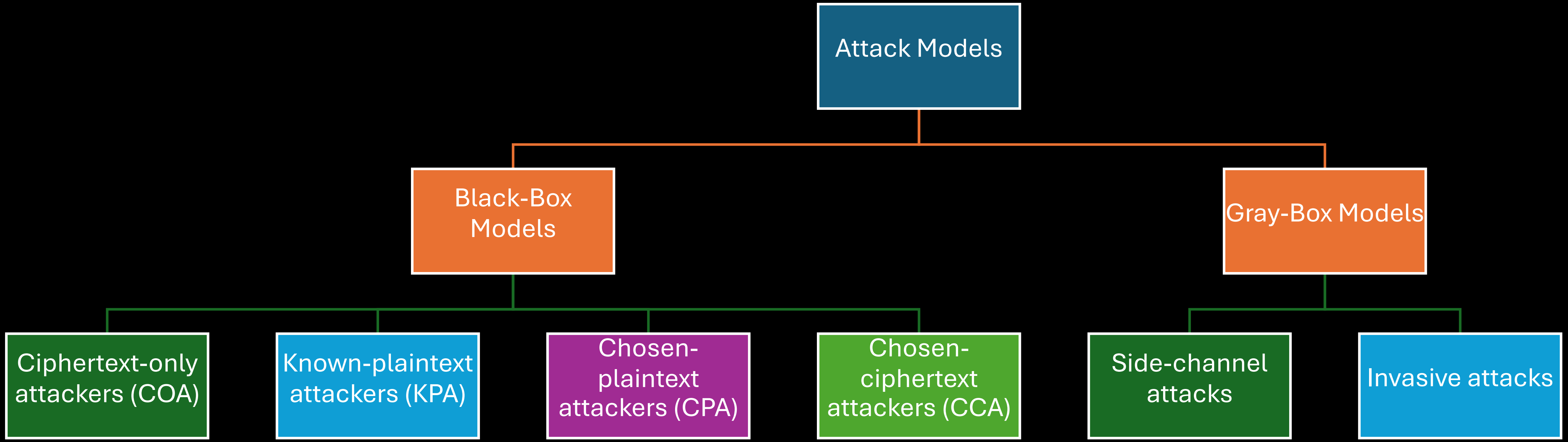
- Security notion = Attack model + Security goal:
  - We say: a cipher achieves <u>a certain security notion</u> if any attacker working in a <u>given model</u> can't achieve the <u>security goal</u>.

Encryption Security: Attack Models

- An attack model is a set of assumptions about how attackers might interact with a cipher and what they can and can’t do.

- Kerkhoff's Principle:
  - The encryption algorithm is known.
  - The security of a cipher rely on the key and the mechanism of the cipher.

Encryption Security: Attack Models



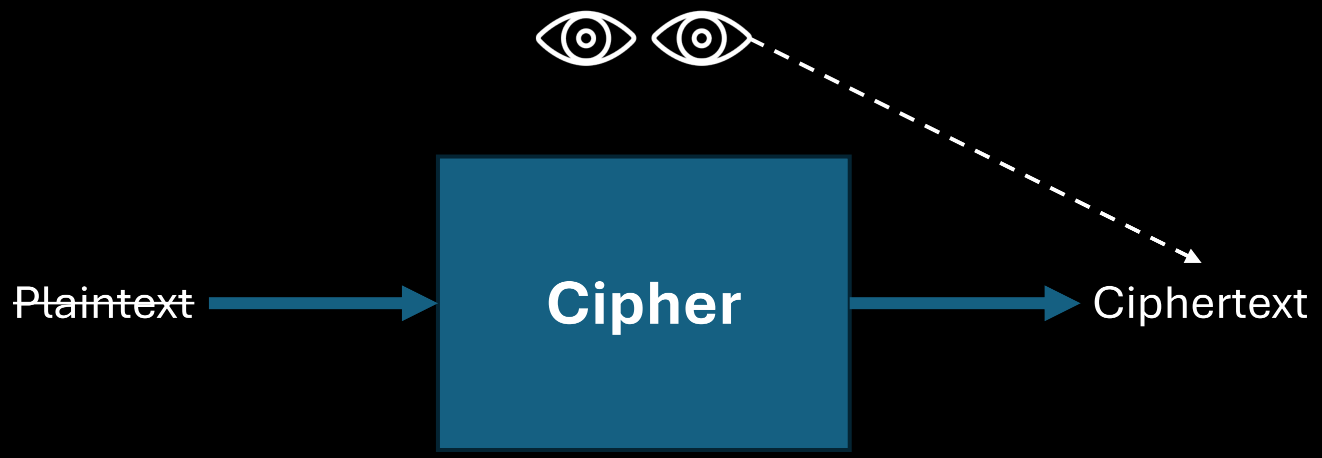
Encryption Security: Attack Models

- In black box models: the attacker can see the input and output of a cipher only.

- In gray box models, the attacker has access to a cipher’s implementation.

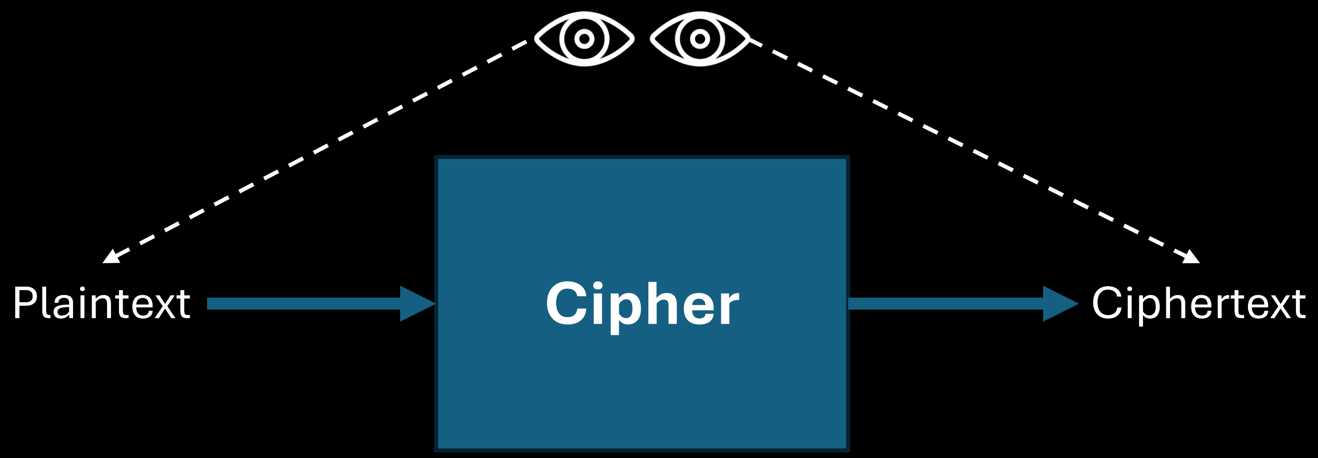
Encryption Security: Attack Models

1. **Ciphertext-only attackers (COA)** observe ciphertexts but don't know the associated plaintexts, and don't know how the plaintexts were selected.
    - Attackers in the COA model are passive and can't perform encryption or decryption queries.



Encryption Security: Attack Models

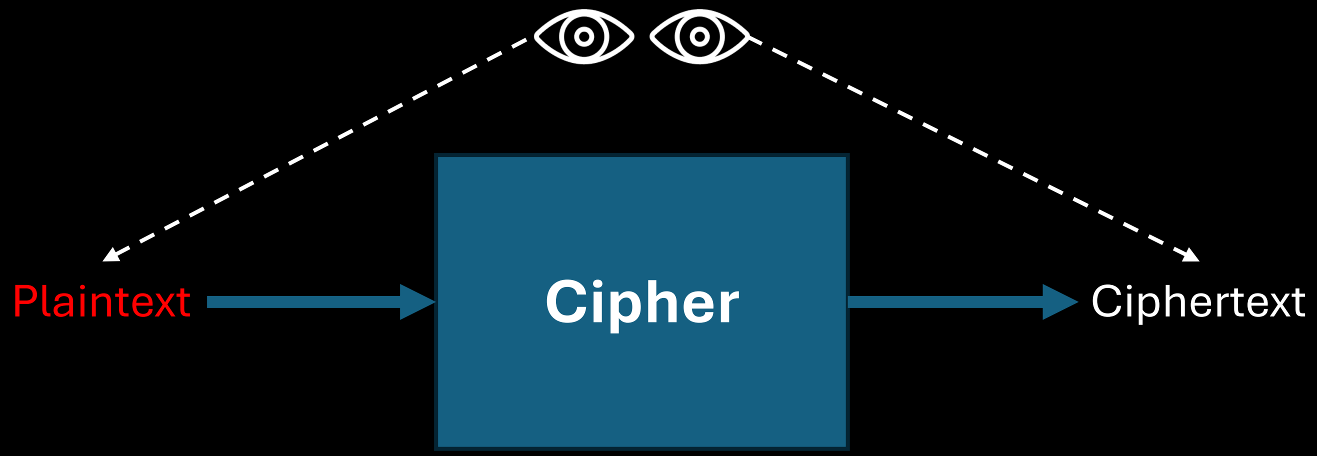
2. **Known-plaintext attackers (KPA)** observe ciphertexts and know the associated plaintexts.
    - Attackers in the KPA model thus get a list of plaintext–ciphertext pairs,
    - KPA is a passive attacker model.



Encryption Security: Attack Models

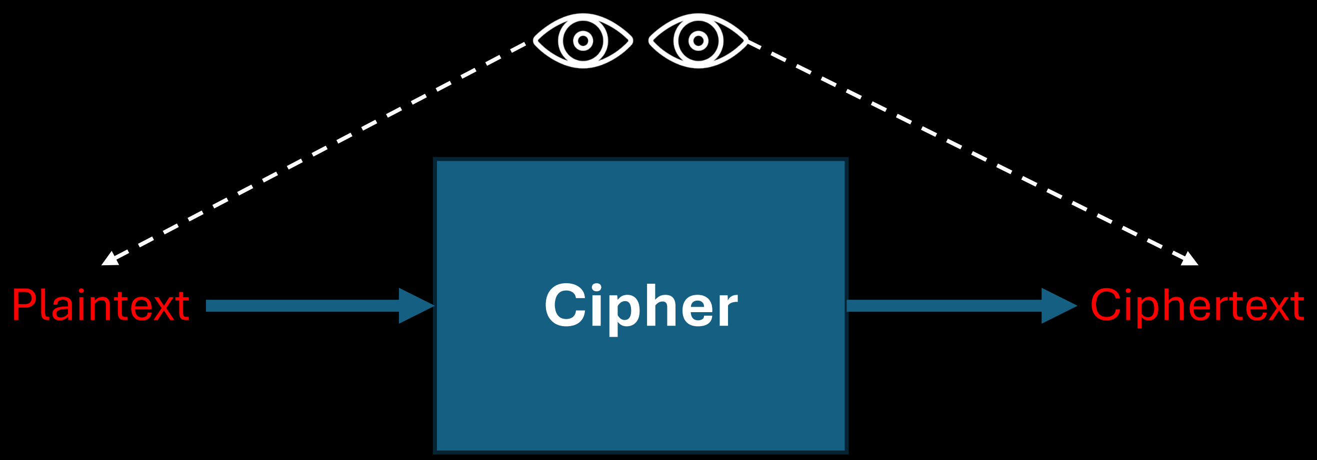
3. **Chosen-plaintext attackers (CPA)** can perform encryption queries for plaintexts of their choice and observe the resulting ciphertexts.

- This model captures situations where attackers can choose all or part of the plaintexts that are encrypted and then get to see the ciphertexts.
- CPA are active attackers, because they influence the encryption processes rather than passively eavesdropping.



Encryption Security: Attack Models

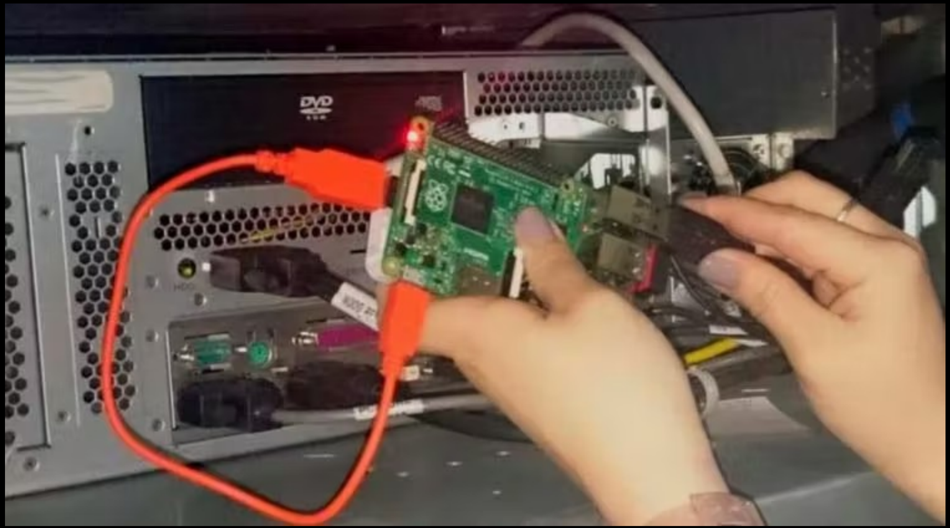
4. **Chosen-ciphertext attackers (CCA)** can both encrypt and decrypt; that is, they get to perform encryption queries and decryption queries.
    - CCA are active attackers



Encryption Security: Attack Models

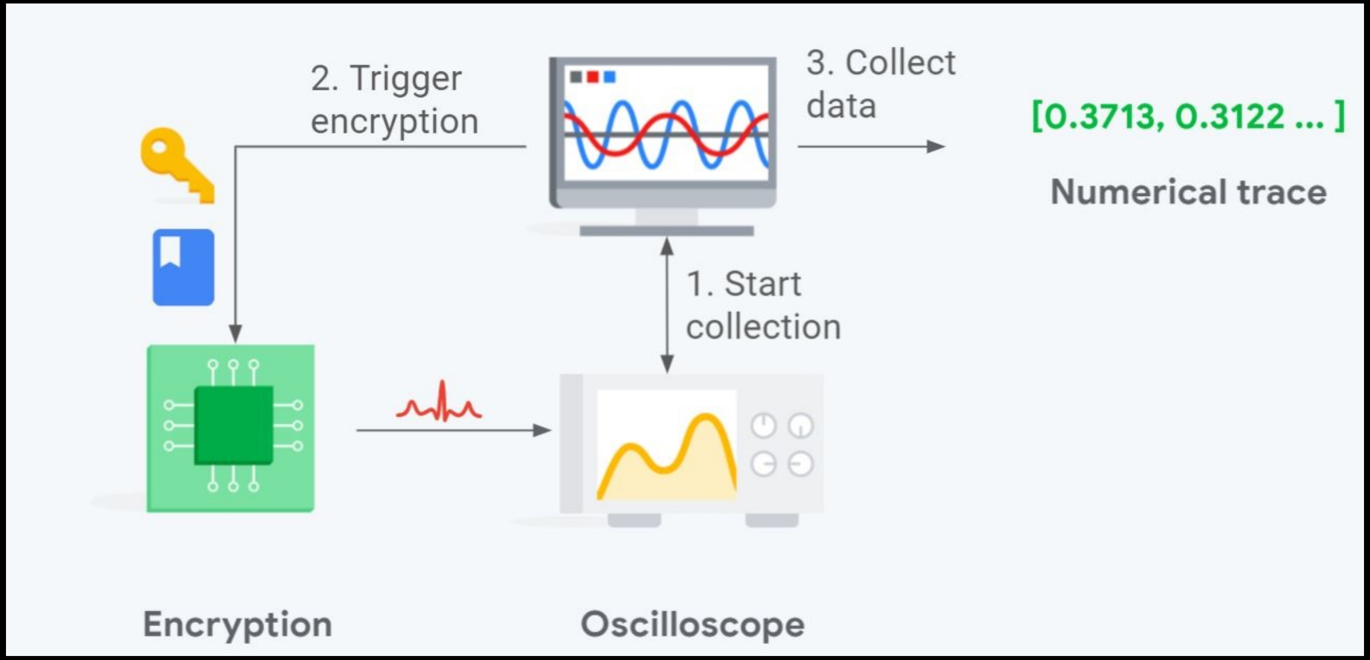
- In gray box models, the attacker has access to a cipher's implementation.
  - It's more realistic for applications such as smart cards, embedded systems, and virtualized systems.
  - Attackers often have physical access and can thus tamper with the algorithms' internals.

Check CSAW-ESC



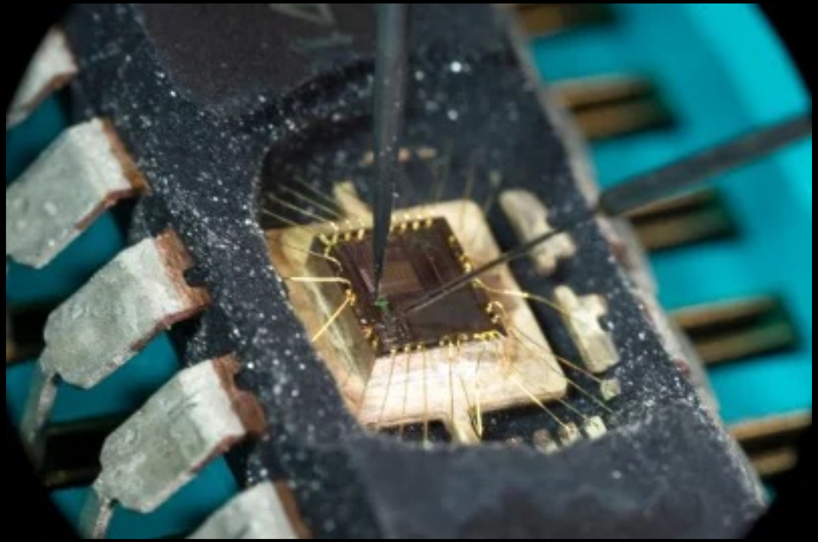
Encryption Security: Attack Models

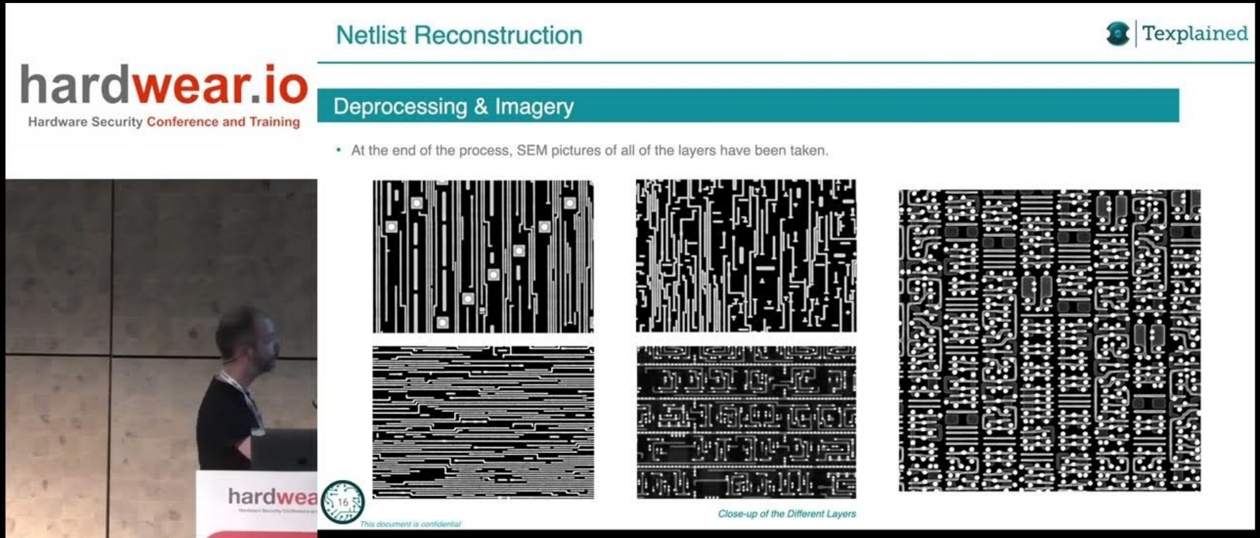
- Gray box models:
  1. **Side-channel attacks.** when an attacker exploits the leakage of physical information from a system during the execution of an application.
     - They are noninvasive.



Encryption Security: Attack Models

- Gray box models:
  2. **Invasive attacks**: require direct access to the internal components of the device, which requires a well-equipped and knowledgeable attacker to succeed.
     - Require tools such as a high-resolution microscopes and a chemical lab.





Practical Invasive Attacks, How The Hardware is Hacked For Compatible Product Creation?
 - Thomas Olivier

Encryption Security: Security Goal

- Security goal: nothing can be learned about the cipher’s behavior.
- Two main security goals:
  1. **Indistinguishability (IND).** Ciphertexts should be indistinguishable from random strings.
  2. **Non-malleability (NM).** Given a ciphertext $C_1 = E(K, P_1)$, it should be impossible to create another ciphertext, C_2, whose corresponding plaintext, P_2, is related to P_1 in a meaningful way.
     - The one-time pad is malleable: given a ciphertext $C_1 = P_1 \oplus K$, you can define $C_2 = C_1 \oplus 1$, which is a valid ciphertext of $P_2 = P_1 \oplus 1$ under the same key K.

Encryption Security: Security Notion

- Security goals are only useful when combined with an attack model.
- The convention is to write a security notion as GOAL-MODEL.
  - IND-CPA
  - IND-CCA
  - NM-CPA
  - NM-CCA

Encryption Security: Security Notion

- The most important one: semantic security – IND-CPA.
- It captures the intuition that ciphertexts shouldn't leak any information about plaintexts as long as the key is secret.
- To achieve IND-CPA security, encryption must return different ciphertexts if called twice on the same plaintext.
  - This is can be achieved using randomized encryption.

Encryption Security: Security Notion

- In IND-CPA, encryption is expressed as $C = E(K, R, P)$
  - C is the result ciphertext
  - E is the encryption function
  - R is fresh random bits
  - K is the secret key
  - P is the plaintext
- Decryption is expressed as $P = D(K, R, C)$

Encryption Security: Security Notion

- To construct a semantically secure cipher, we can use a deterministic random bit generator (DRBG).

- A DRBG is an algorithm that returns random looking bits given some secret value.

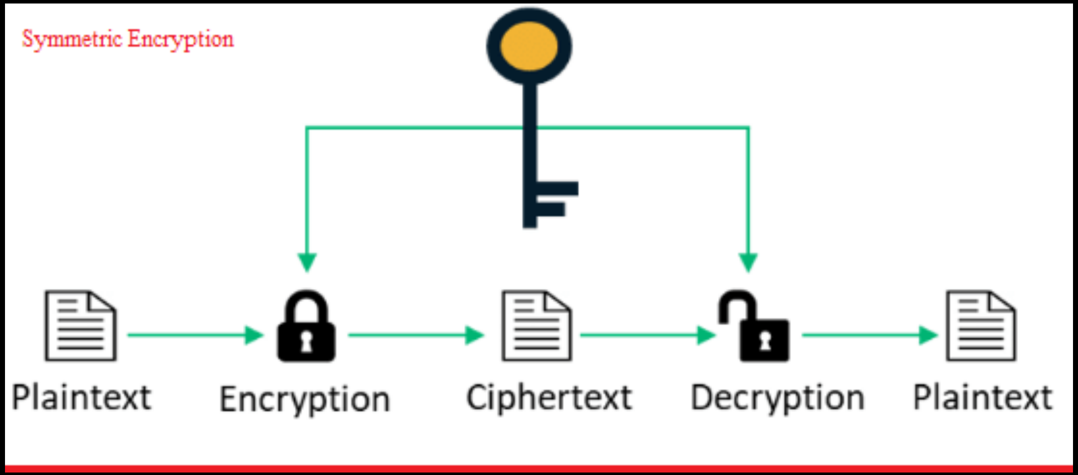
$$E(K, R, P) = (DRBG(K||R) \oplus P, R)$$

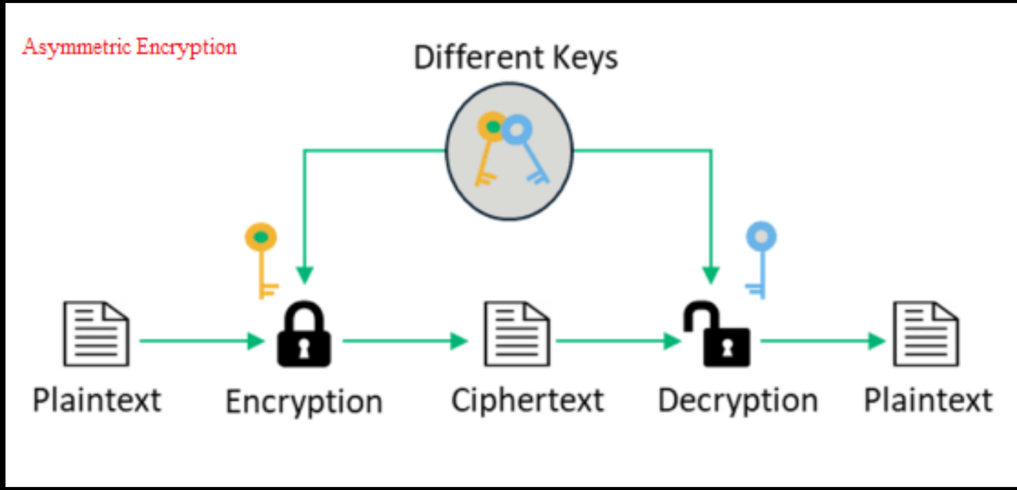
  - $K||R$ means concatenating the key with random bits.

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

Asymmetric Encryption

- The previous are symmetric ciphers, where two parties share a key.
- In asymmetric encryption, there are two keys:
  - The **encryption** key (**public key**),publicly available to anyone who wants to send you encrypted messages.
  - The **decryption** key must remain secret and is called a **private** key.





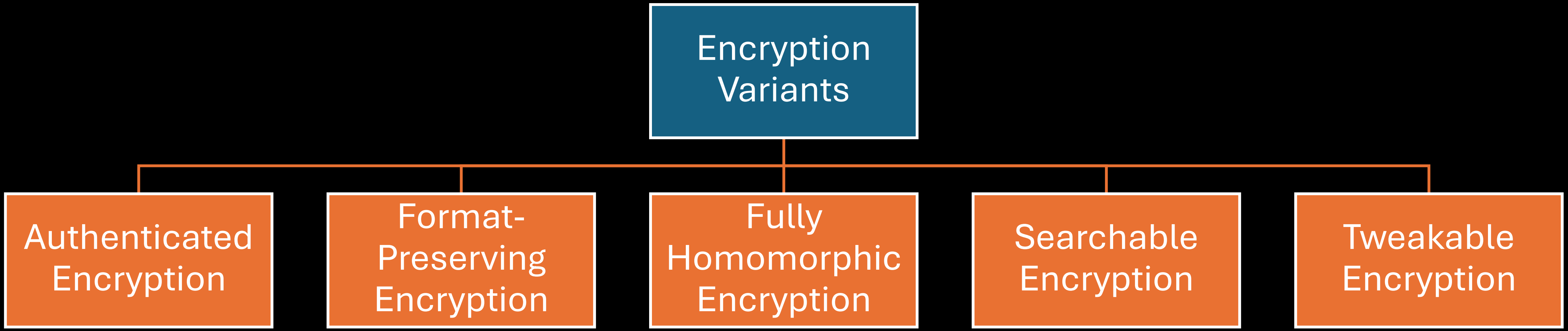
Asymmetric Encryption

- The public key can be computed from the private key,
-
- The private key can’t be computed from the public key.

- The point of public key cryptography is that you can compute the functions in one direction but practically impossible to invert.

Content
Introduction
Caesar Cipher
Vigenère Cipher
How Ciphers Work
The Permutation
Modes of Operations
The One-time Pad
Encryption Security
Asymmetric Encryption
When Ciphers Do More Than Encryption

When Ciphers Do More Than Encryption



When Ciphers Do More Than Encryption

Authenticated Encryption:

- A symmetric encryption that returns an authentication tag and a ciphertext.
- AE(K, P) = (C, T)
  - the tag T is a short string that's impossible to guess without the key.
- The tag ensures the integrity of the message.
  - evidence that the ciphertext received is identical to the one sent in the first
- Decryption takes K, C, and T and returns P only if it verifies that T is valid otherwise, it aborts and returns some error.

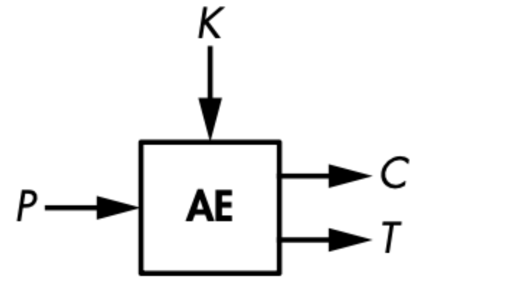


Figure 1-4: Authenticated encryption

When Ciphers Do More Than Encryption

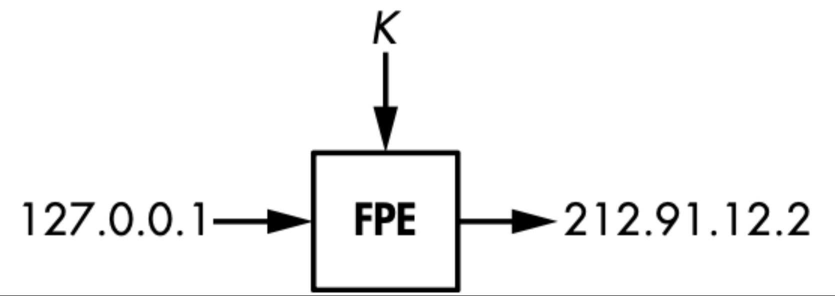
Authenticated encryption with associated data (AEAD):

- An extension of authenticated encryption that takes some cleartext and unencrypted data and uses it to generate the authentication tag.
- AEAD(K, P, A) = (C, T).
- Can be used to protect protocols’ datagrams with a cleartext header and an encrypted payload.
  - Destination addresses need to be clear in order to route network packets.

When Ciphers Do More Than Encryption

Format-Preserving Encryption:

- It can create ciphertexts that have the same format as the plaintext.
- For example, FPE can encrypt
  - IP addresses to IP addresses
  - ZIP codes to ZIP codes,
  - credit card numbers to credit card numbers



When Ciphers Do More Than Encryption

Fully Homomorphic Encryption:

- Enables computing a function on a ciphertext without the need to decrypting it.
- In FHE:
  - If we need to compute a function F on a plaintext P to get a result.
  - FHE encrypts P to C and transforms F to F`.
  - Then compute F`(C) to C`.
  - When decrypting C`, we get F(P).
- Downside: very slow.

When Ciphers Do More Than Encryption

Searchable Encryption:

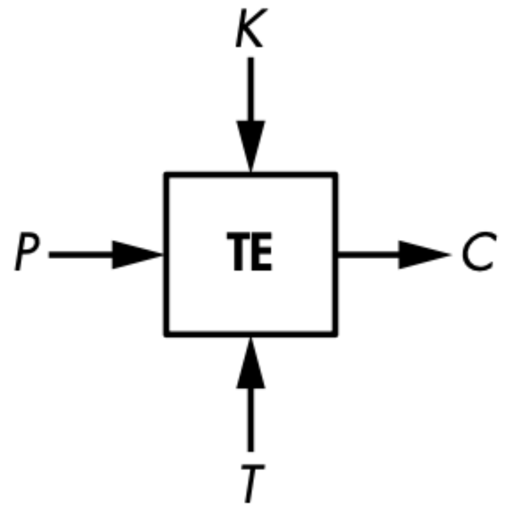
- Enables searching over an encrypted database without leaking the searched terms by encrypting the search query itself.

- FHE and searchable encryption can enhance the privacy of many cloud-based applications by hiding your searches from your cloud provider.

When Ciphers Do More Than Encryption

Tweakable Encryption:

- Similar to basic encryption, except it has a parameter called a *tweak*.
  - aims to simulate different versions of a cipher.



- The main application is disk encryption.
  - It uses a tweak value that depends on the position of the data encrypted, which is usually a sector number or a block index.