التشفير واستخداماته

تعرف على أهمية التشفير وكيفية استخدامه في مختلف المجالات.

Dr Mohammed Alshahrani

مقدمة للتشفير

تعريف التشفير

التشفير هو تحويل المعلومات إلى شكل مشفر لحمايتها.

أهمية التشفير

التشفير أصبح ضروريًا في العصر الحديث لحماية البيانات.

تطبيقات التشفير

يستخدم التشفير في مجالات مثل الأمن السيبراني والتجارة الإلكترونية.

لمحة تاريخية

1

العصور القديمة

التشفير موجود منذ آلاف السنين

2

العصور الوسطى

تطور أساليب التشفير التقليدية

3

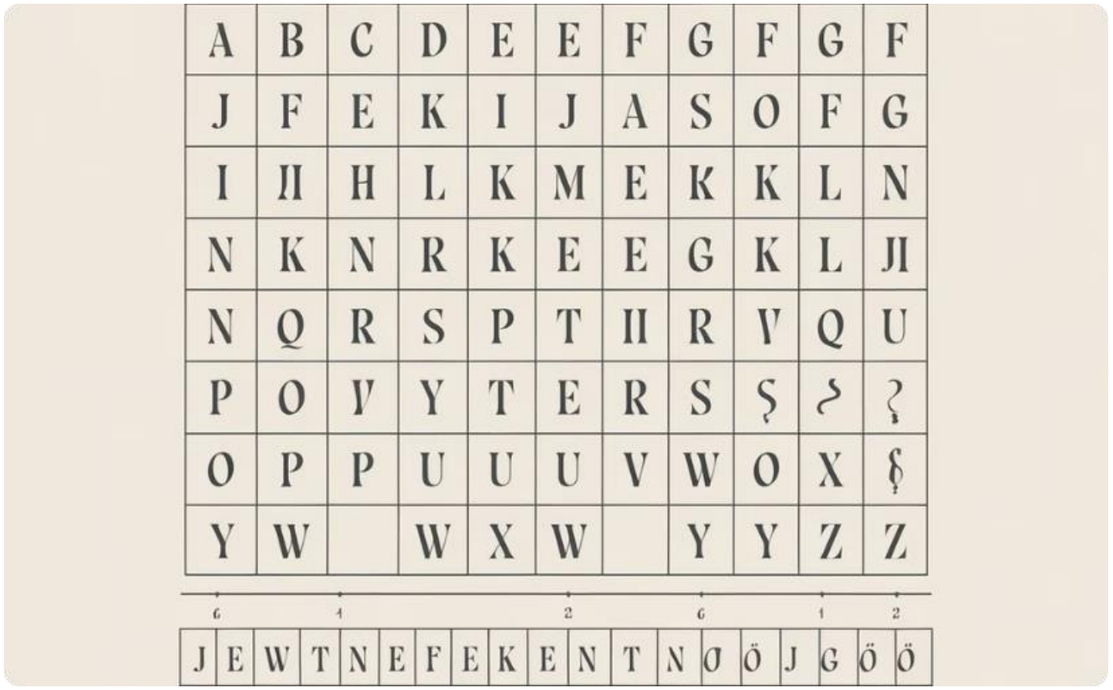
العصر الحديث

ظهور التشفير الرقمي والتكنولوجي

التشفير التقليدي

شيفرة قيصر

تبديل الحروف بحسب قاعدة ثابتة



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

6	4	2	6	1	2
J	E	W	T	N	E	F	E	K	E	N	T	N	ʊ	Ö	J	G	Ö	Ö

شيفرة فيجينير

استخدام مفتاح متغير لتشفير الرسالة

Simple Substitution

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext	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
Ciphertext	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

Ciphertext:

IRXUVFRUHDQGVHYHQBHDUVDJR

Shift by 3 is “Caesar’s cipher”

Caesar's Cipher Decryption

- Suppose we know a Caesar's cipher is being used:

Plaintext	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
Ciphertext	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

- Given ciphertext:

VSRQJHEREVTXDUHSDQWV

- Plaintext: spongebobsquarepants

Not-so-Simple Substitution

- Shift by n for some $n \in \{0,1,2,\ldots,25\}$
- Then key is n
- Example: key $n = 7$

Plaintext	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
Ciphertext	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

مثال على شيفرة فيجينر (Vigenère Cipher):

- النص الأصلي: HELLO
- يجب تكرار المفتاح ليتطابق مع طول النص:
- التشفير:
- H + K = (7 + 10) % 26 = 17 → R
- E + E = (4 + 4) % 26 = 8 → I
- L + Y = (11 + 24) % 26 = 9 → J
- L + K = (11 + 10) % 26 = 21 → V
- O + E = (14 + 4) % 26 = 18 → S
- النص المشفَّر: RIJVS

المفتاح: KEY

النص الأصلي: HELLO المفتاح: KEYKE

مثال على شيفرة فيجينر :(Vigenère Cipher)

- فك التشفير:
- نقوم بطرح قيمة الحرف في المفتاح من الحرف المشفر:

- R - K = (17 - 10) % 26 = 7 → H
- I - E = (8 - 4) % 26 = 4 → E
- J - Y = (9 - 24 + 26) % 26 = 11 → L
- V - K = (21 - 10) % 26 = 11 → L
- S - E = (18 - 4) % 26 = 14 → O
- النص المفكوك: HELLO

التشفير الحديث

الحوسبة

تطبيق التشفير في الأنظمة الحاسوبية.

الانتقال

الانتقال من التشفير التقليدي إلى الرقمي.

التشفير الرقمي

استخدام التشفير في الحوسبة الرقمية.

أنواع التشفير

التشفير غير المتناظر

استخدام مفتاحين منفصلين للتشفير والفك.

التشفير المتناظر

استخدام مفتاح واحد للتشفير والفك.

التشفير المتناظر

1

التشفير المتناظر

استخدام مفتاح واحد للتشفير والفك

2

أمثلة

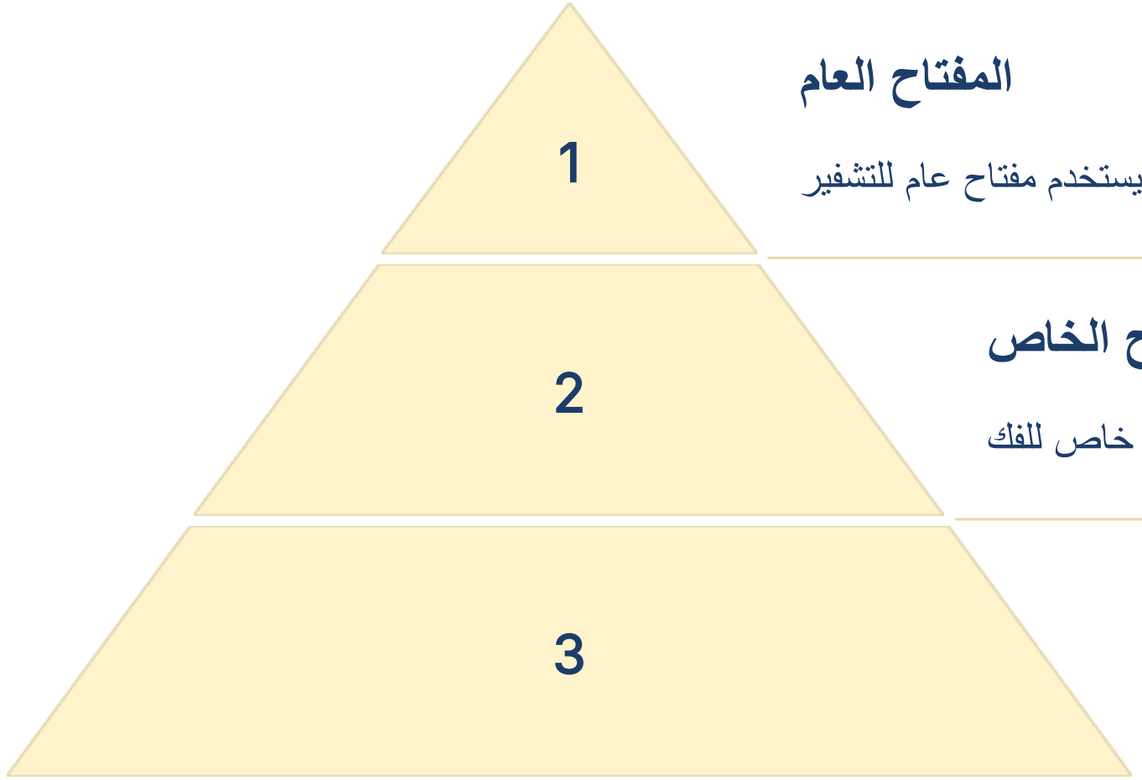
Twofish ،Blowfish ،DES ،AES

3

الخصائص

سرعة عالية، تشفير وفك سريع

التشفير غير المتناظر



المفتاح العام

يستخدم مفتاح عام للتشفير

المفتاح الخاص

يستخدم مفتاح خاص للفك

RSA

مثال على تشفير غير متناظر

يعمل التشفير غير المتناظر باستخدام مفتاحين منفصلين :مفتاح عام للتشفير ومفتاح خاص لفك التشفير .أحد الأمثلة الشائعة على هذا النوع من التشفير هو نظام .RSA

المفتاح العام والمفتاح الخاص

المفتاح العام

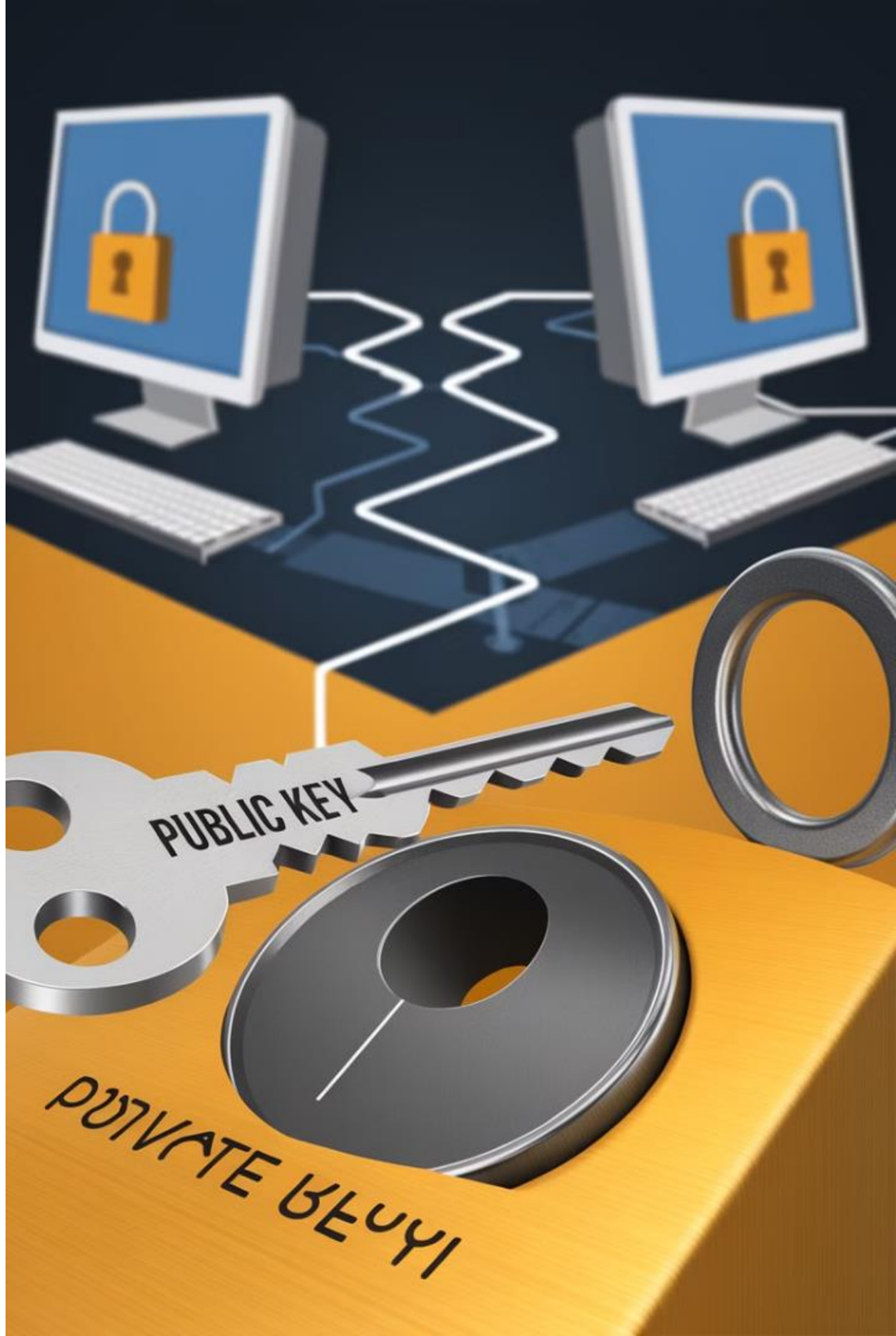
يُستخدم للتشفير والتحقق من الهوية

المفتاح الخاص

يُستخدم لفك التشفير والتوقيع الرقمي

الاستخدام المتكامل

المفتاحان يعملان معًا لضمان الأمان



الشهادات الرقمية

دور الشهادات الرقمية

تضمن الشهادات الرقمية أمن التشفير.

تأكيد الهوية

تستخدم الشهادات لتأكيد هوية المستخدم.

حماية البيانات

تضمن الشهادات سرية وسلامة البيانات.

SSL/TLS

الحماية

توفير الحماية للبيانات المنقولة.

الاتصال الآمن

ضمان الاتصال الآمن عبر الإنترنت.

التشفير الآمن

بروتوكولات الاتصال الآمن على الإنترنت.

التشفير في بروتوكولات الاتصال الآمن على الإنترنت

1

SSL/TLS

بروتوكولات الاتصال الآمن على الإنترنت

2

التشفير

يضمن سرية وسلامة البيانات المنقولة

3

الاتصال الآمن

يحمي المستخدمين من التجسس والاختراق

تشفير البريد الإلكتروني

PGP

استخدام PGPلتشفير البريد الإلكتروني.

الخصوصية

حماية البيانات الحساسة في البريد الإلكتروني.

الأمان

تأمين الاتصالات البريدية من التجسس والاختراق.

التشفير في الهواتف المحمولة

الخصوصية

الحفاظ على خصوصية المستخدمين في الهواتف المحمولة.

حماية البيانات

استخدام التشفير لحماية بيانات الهواتف المحمولة.

التشفير في الشبكات الافتراضية الخاصة (VPN)

حماية الاتصال

VPNتستخدم التشفير لحماية الاتصال.

شبكة آمنة

VPNتوفر شبكة افتراضية خاصة وآمنة.

الخصوصية

VPNتحمي خصوصية المستخدم أثناء التصفح.

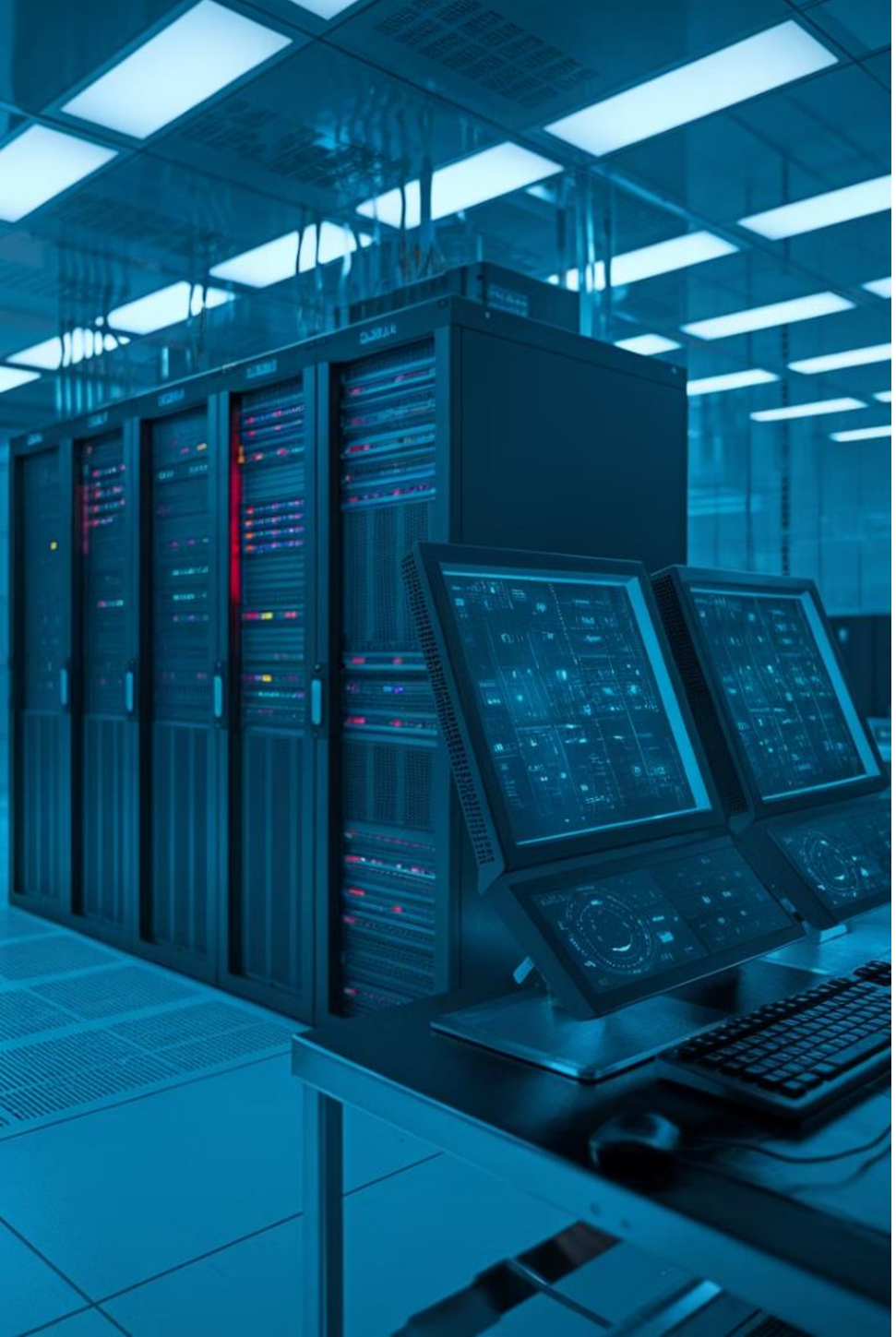
تشفير البيانات المخزنة

تطبيقات التشفير

تخزين السجلات الطبية والملفات المالية.

أهمية التشفير

حماية البيانات الحساسة المخزنة.



التشفير وتخزين البيانات

حماية البيانات الحساسة

التشفير يضمن أمان البيانات المخزنة.

الخصوصية والأمان

التشفير يحمي البيانات من الوصول غير المصرح به.

الامتثال التنظيمي

التشفير يساعد في تلبية متطلبات الخصوصية والأمان.

التشفير في التجارة الإلكترونية

حماية المعاملات المالية

استخدام التشفير لحماية المعاملات المالية عبر الإنترنت.

التشفير في الحوسبة السحابية

1

حماية البيانات

تشفير البيانات المخزنة في السحابة.

تشفير الهوية والبلوك تشين

تأمين الهوية

التشفير يؤمن هوية المستخدم في البلوك تشين.

تأمين المعاملات

التشفير يؤمن المعاملات في تقنية البلوك تشين.

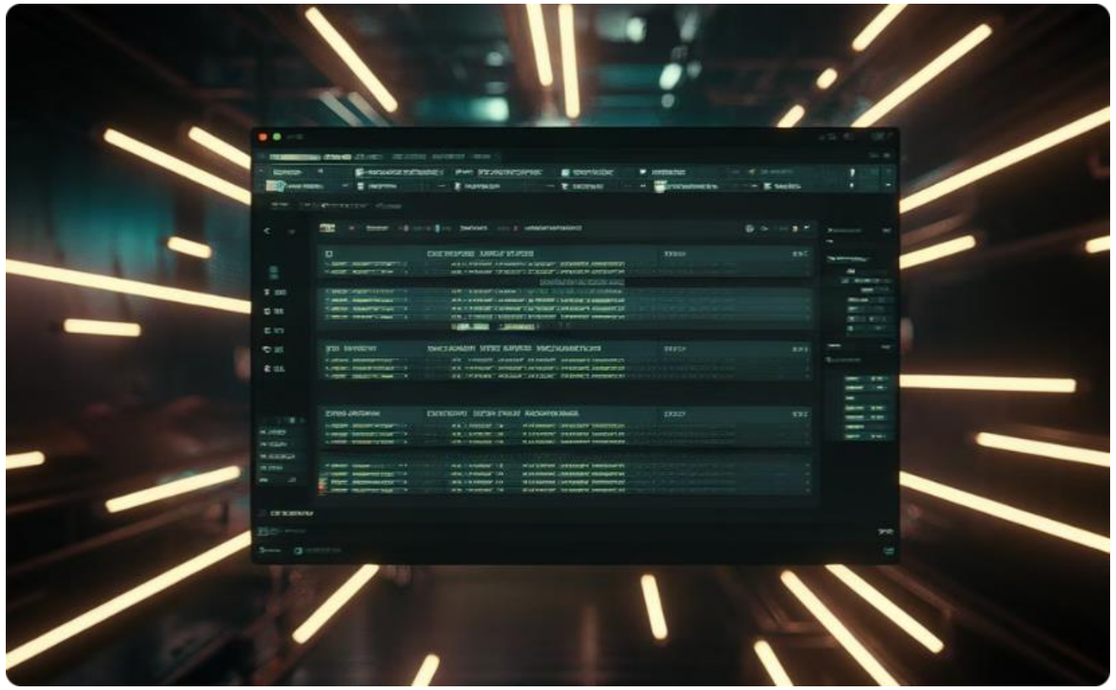
تقنية البلوك تشين

التشفير يلعب دورًا أساسيًا في تقنية البلوك تشين.

التشفير في الإنترنت المظلم

تأمين الاتصال

التشفير يؤمن الاتصالات في الإنترنت المظلم.



إخفاء الهوية

التشفير يساعد على إخفاء الهوية في الإنترنت المظلم.

الهجمات على التشفير

هجوم الرجل في المنتصف (MITM)

هجوم شائع يستهدف التواصل المشفر بين طرفين.

الهجمات الأخرى

مثل هجمات القوة البرية والهجمات الإحصائية.

الحماية من الهجمات

استخدام بروتوكولات آمنة وتحديث البرامج.

التشفير الكمي والخصوصية

الاستخدامات المستقبلية

حماية البيانات الحساسة من الاختراق.

التشفير الكمي

تقنية جديدة لتعزيز أمن البيانات.

تحديات التشفير الكلاسيكي

التقدم التقني

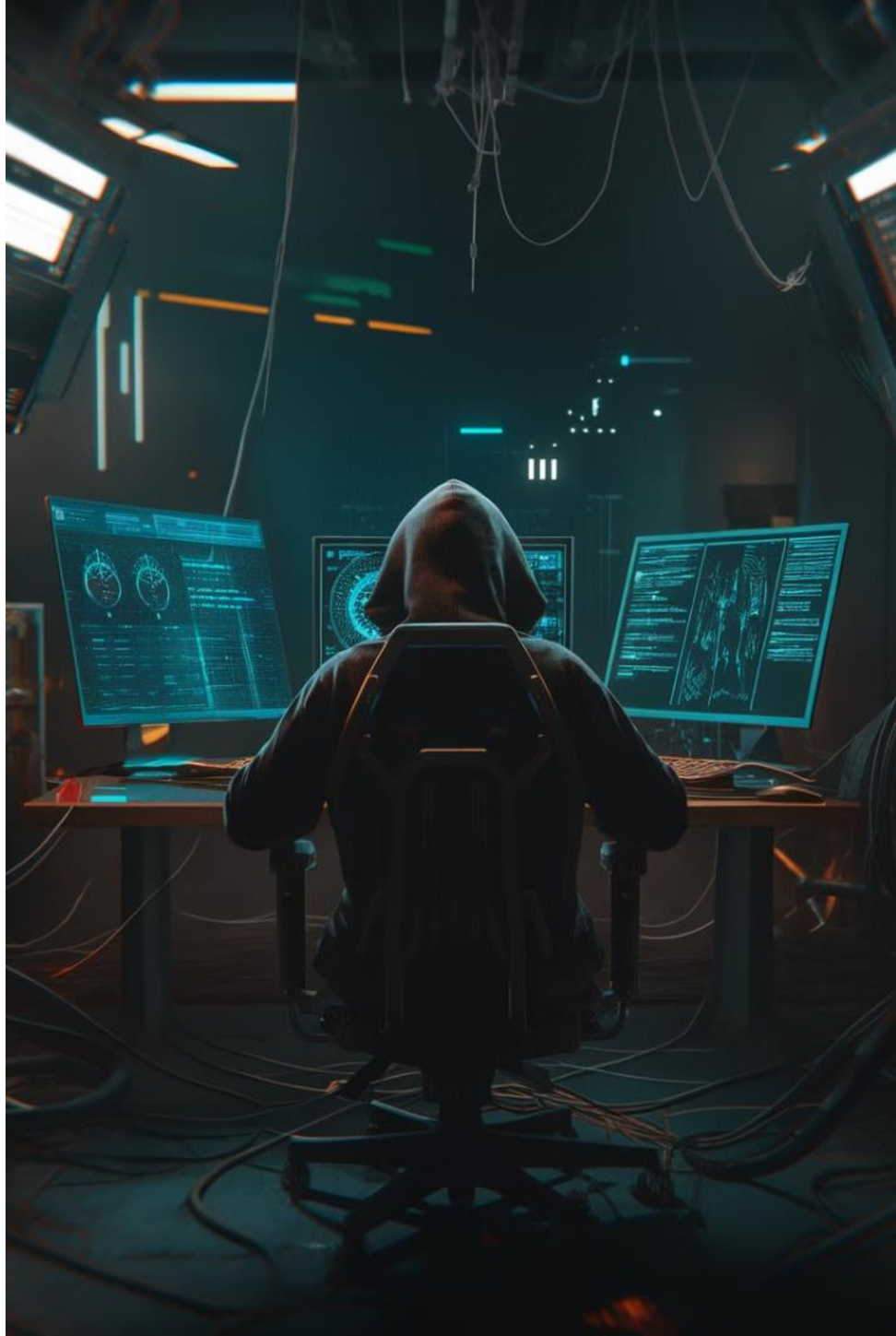
التحديات مع التطور التكنولوجي المتسارع.

قوة الحوسبة

زيادة قوة الحوسبة تشكل تهديدًا للتشفير التقليدي.

الهجمات الحديثة

ظهور هجمات متطورة تستهدف التشفير الكلاسيكي.



قوانين التشفير والخصوصية

القوانين المنظمة

قوانين تنظم استخدام التشفير وحماية الخصوصية.

حماية الخصوصية

التشفير يلعب دوراً حيوياً في حماية الخصوصية.

التوازن

التوازن بين التشفير والخصوصية والأمن.