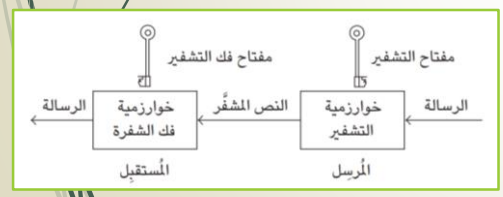
GS224 - 5

التشفـــــــير (Encryption)

التشفير (Encryption)

التشفير هو أحد تقنيات العمل الأساسية المستخدمة في مجال أمن المعلومات. فالتشفير يساعد بشكل أساسي على الحفاظ على سرية المعلومات. ومن خال تطبيقات ُمبتكرة يمكن للتشفير أيضاً ُ التأكد من تكامل المعلومات والتأكد من هوية المرسل. وكل العمليات التجارية التي يتم إجراؤها عبر الإنترنت تستخدم التشفير للحفاظ على أمن المعلومات. ويضمن التشفير أن المعلومات المالية، مثل أرقام بطاقات الائتمان، المرسلة عبر شبكة الإنترنت لا يتم سرقتها أثناء عملية النقل. وفي كثير من الحالات فإن التشفير ليس أمراً مناسباً فقط بل هو أمر مطلوب بموجب القانون الوطني، لذا فإن التشفير جزء أساسي من البنية التحتية التجارية و الإدارية الحديثة.

غالبًا ما يطلَق على المعلومات المراد إخفاؤها اسم «النص الصريح»، فيما يطلق على عملية إخفائها اسم «التشفير». ويطلق على النص الأصلي المشفَّر اسم «النص المشفَّر» أو «بيان التشفير»، كما يطلق على مجموعة القواعد المستخدمة في تشفير معلومات النص الصريح «خوارزمية التشفير». عادةً، تعتمد هذه الخوارزمية على «مفتاح التشفير» ؛ وهو ً يمثل مدخلا لها بالإضافة إلى الرسالة. وحتى يتمكن المتلقي من استرجاع الرسالة من خلال النص المشفر، يجب أن تتوافر «خوارزمية فك التشفير» التي، عند استخدامها مع «مفتاح فك التشفير» المناسب، تسترجع النص الصريح من النص المشفَّر.



يطلق على كل من يعترض رسالة خلال انتقالها اسم «معترض» ، وربما أسماء أخرى، مثل «متنصت»، و«خصم»، و«غريم»، و«شخص سيئ». إلا أنه يجب الإشارة إلى أن المعترضين يمكن أن يكونوا «أشخاصا طيبين» في بعض الأحيان. وحتى إن علم المعترضون بخوارزمية فك التشفير، فإنهم في العموم لا يعرفون مفتاح فك التشفير. ومن المأمول أن تَمنع عدم المعرفة هذه المعترضين من معرفة النص الصريح. وعلم «التشفير» هو علم تصميم أنظمة التشفير، بينما يشير «تحليل الشيفَّرة» إلى العملية التي يجري من خلالها استنباط المعلومات حول النص الصريح دون معرفة مفتاح التشفير المناسب.

التشفير : التصنيف

تصنف نظم التشفير على الأسس التالية :

1. **اسلوب عملية التشفير** : حيث تعتمد كل عمليات التشفير على النقل أو التبديل. في عمليات التبديل يتم استبدال أي عنصر في النص الصريح (خانة او حرف او مجموعة خانات او ثنائيات .... الخ) بعنصر اخر محدد مناظر له. اما في عملية النقل فيتم إعادة ترتيب العناصر في النص الصريح مع عدم إضاعة أي عنصر، حتى تكون كل العمليات عكسية. وقد تتضمن عملية التشفير عدة مراحل من التبديل و النقل.
2. **عدد المفاتيح المستخدمة** : عند استخدام كل من المرسل و المستقبل نفس المفتاح يطلق على نظام التشفير نظام التشفير المتناظر أو التشفير بالمفتاح السرى. اما اذا استخدام كل من المرسل و المستقبل مفتاحين مختلفين عن بعضهما البعض فيسمى نظام التشفير غير المتناظر او التشفير بالمفتاح العام. كما توجد طرق تشفير لا تستخدم مفتاح لتشفير المعلومات حيث الفكرة الأساسية هي أن قيمة التشفير الناتجة تمثل صورة مختصرة للرسالة الأصلية.
3. **طريقة معالجة النص الصريح** : قد يعالج النص الصريح في عملية التشفير على هيئة كتل ، في كل مرة تعالج كتلة واحدة من العناصر، مما ينتج في الخرج كتلة (مشفرة) تتوافق مع كتلة الدخل (صريحة) و يعرف بالتشفير الكتلي (Block cipher). كما يمكن ان تتم المعالجة بحيث يتم التعامل مع الدخل في عملية التشفير وفق تدفق للعناصر على التوالي ، عنصر واحد في أي وقت ، مما ينتج عنه خرجا على شكل سلسلة ، ويعرف بالتشفير التدفقي (Stream cipher).

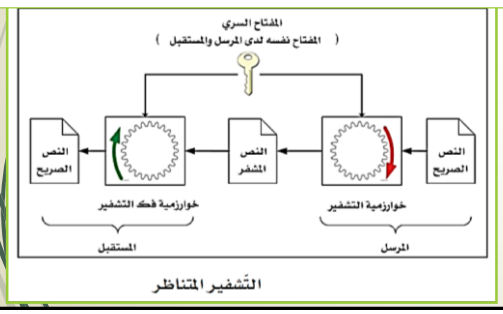
1 – التشفير بالمفتاح السري (التناظري) : الالية

يشير التشفير بالمفتاح السري إلى طرق التشفير التي تستخدم مفتاحاً واحداً لكل من التشفير وفك التشفير. ويقدم الشكل لمحة عامة عن التشفير بالمفتاح السري.

وكما نرى في الشكل فإن السمة الأساسية في التشفير بالمفتاح السري هي استخدام المفتاح نفسه لكل من التشفير وفك التشفير. ونتيجة لهذا التماثل في المفاتيح المستخدمة في التشفير وفك التشفير، تسمى طريقة التشفير بالمفتاح السري "التشفير بالمفتاح المتناظر" (Symmetric Key Encryption) أو (Symmetric Key Cryptography) ، ويستخدم التشفير بالمفتاح السري بشكل شائع في نقل المعلومات بشكل آمن. فإذا اتفق كل من طرفي الاتصال (س و ص) على استخدام مفتاح موحد، فإن (س) يستطيع تشفير معلوماته بهذا المفتاح كما يستطيع (ص) فك تشفير المعلومات باستخدام المفتاح نفسه. وبالمثل فإن بإمكان (س) تشفير معلوماته بالمفتاح المشترك وبإمكان (ص) كذلك فك تشفير المعلومات باستخدام المفتاح المشترك نفسه. وستكون المعلومات آمنة أثناء الإرسال لأن (ص) و (س) فقط يعرفان المفتاح ، فإنه يكاد يكون من المستحيل فك تشفير المعلومات المرسلة دون معرفة المفتاح.

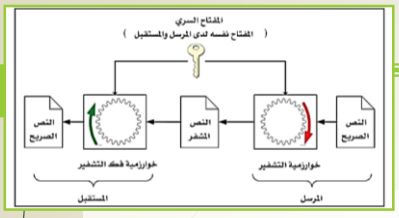
وتتم عمليتا التشفير و فك التشفير كالتالي:

- **عملية التشفير**: تشفر الرسالة الأصلية باستخدام خوارزمية التشفير والمفتاح السري المشترك للحصول على رسالة مشفرة.
- **عملية فك التشفير**: يفك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح السري المشترك للحصول على الرسالة الأصلية.



التَشفير المتناظر

1 – التشفير بالمفتاح السري (التناظري)



- ويمكن أيضاً استخدام التشفير بالمفتاح السري لتأمين المعلومات المحفوظة في أجهزة الحاسوب. فإذا أراد (س) تأمن بعض المعلومات، عليه اختيار المفتاح ومن ثم تشفير المعلومات المحفوظة في القرص الصلب باستخدام ذلك المفتاح. واسترجاع المعلومات، على (س) أن يقوم بإدخال المفتاح وفك تشفير المعلومات. وبطبيعة الحال، إذا نسي (س) المفتاح فلن يكون قادراً على استرجاع المعلومات المحفوظة في جهاز حاسوبه.
- المعيار الحالي للتشفير بالمفتاح السري هو معيار التشفير المتقدم (**A**dvanced **E**ncryption **S**tandard) - (**AES**). تم اختيار هذا المعيار من قبل المعهد الوطني للمعايير والتقنية (National Institute for Technology and Standards). ومن التقنيات السابقة لمعيار التشفير المتقدم تقنية معيار تشفير البيانات الثلاثي (**3** **D**ata **E**ncryption **S**tandard)، وخوارزمية تشفير البيانات الدولية (**I**nternational **D**ata **E**ncryption **A**lgorithm).

1 – التشفير بالمفتاح السري (التناظري) : المكونات

1. **النص الصريح**: وهو النص أو الرسالة الأصلية المقروءة التي يجري إدخالها إلى خوارزمية التشفير.
2. **خوارزمية التشفير**: وهي الطريقة التي تشتمل على مجموعة الخطوات التي يتم تنفيذها على النص الصريح لإنتاج النص المشفر باستخدام المفتاح السري. وتتكون مدخلات خوارزمية التشفير من النص الصريح، والمفتاح السري ومخرجاتها من النص المشفر. ومن أشهر خوارزميات التشفير : AES , 3DES.
3. **المفتاح السري**: وهو المفتاح الذي يتم إدخاله إلى خوارزمية التشفير (بالإضافة إلى النص الصريح) لإنتاج النص المشفر. وهو عبارة عن قيمة يتم اختيارها من قبل المستخدم أو إنتاجها من قبل النظام (مستحسن)، وهي نفس القيمة التي تستخدم في التشفير وفك التشفير. وفي كل مرة يجرى فيها اختيار مفتاح مختلف ينتج نص مشفر مختلف، حتى ولو كان للنص الصريح نفسه.
4. **النص المشفر**: وهو الرسالة التي تنتجها خوارزمية التشفير من كل من النص الصريح والمفتاح السري.
5. **خوارزمية فك التشفير**: وهي خوارزمية التشفير نفسها ولكن تعمل بشكل عكسي لها ، وتتكون مدخلات خوارزمية فك التشفير من النص المشفر والمفتاح السري، ومخرجاتها من النص الصريح.

1 – التشفير بالمفتاح السري (التناظري) : الآمان

للحصول على التشفير متناظر آمن، يجب تحقيق :

1. استخدام خوارزمية تشفير (وفك التشفير) قوية ، و الخوارزمية القوية هي التي لا يمكن ارجاع النصوص المشفرة المنتجة منها الى نصوص صريحة، حتى ولو كانت الخوارزمية نفسها معروفة عند من يحاول فك التشفير (المعتدي). و عموما فإن خوارزمية التشفير القوية هي التي يكون المعتدي عليها غير قادر على فك تشفير النص المشفر أو اكتشاف المفاتيح السرية، حتى لو توفرت لديه عدد من النصوص الصريحة و النصوص المشفرة المناظرة لها.
2. يجب توزيع المفتاح على كل من المرسل و المستقبل بشكل آمن ، و أن يبقى هذا المفتاح سريا بينهما. فلو حصل أحد على المفتاح السري فإنه سيصبح بإمكانه فك التشفير الرسائل المشفرة باستخدام خوارزمية التشفير التي عادة ما تكون معرفة للجميع.
3. ضمان سرية المفتاح السري و قوته :
   - انتاج مفاتيح السرية بشكل آلي من قبل النظام و ليس من قبل المستخدم.
   - استخدام مفاتيح عشوائية مختلفة لكل عملية ارسال مختلفة.
   - استخدام مفاتيح سرية طويلة لا تقل عن 256 خانة ثنائية (بت).
   - استخدام مفاتيح سرية في صيغتها الثنائية (0،1) فقط و ليست في صيغتها الأبجدية المعتادة (احرف و ارقام).

1 – التشفير بالمفتاح السري (التناظري) : تحليل التشفير

هناك طريقتان يمكن استخدامهما لاكتشاف النص الصريح و فك تشفير الرسالة المشفرة دون معرفة نظام التشفير المستخدم او مفتاح السرى مسبقا، وهما:

1. **تكسير التشفير**: ويعتمد على تحليل التشفير بناء على خوارزمية معينة و الاعتماد على بعض معطيات النص الصريح المعروفة للمحلل (المهاجم) لاستنتاج النص الصريح او استنتاج المفتاح المستخدم. ويتطلب هذا الأسلوب ان تكون خوارزمية التشفير معروفة للمحلل، وقد يستخدم بعض الخصائص الإحصائية للغة المستخدمة للحصول على النص الصريح او المفتاح، او ربما يستغل نسق معين في النص المشفر.
2. **هجوم التكسير الاعمى او البحث الشامل**: وفيه يحاول المهاجم تجريب كل المفاتيح المحتملة على مقطع من النص المشفر و يستمر في هذه المحاولات حتى يتحصل على نص صريح مفهوم وواضح. في هذه الأسلوب كلما زاد طول المفتاح اصبح كسر الشفرة اكثر صعوبة، و ان الزمن المطلوب لتحليل الشفرة بهذه الطريقة يعتمد بدرجة كبيرة على مقدرات الحاسوب المستخدم.

يعتبر أسلوب التشفير "امنا بشكل مطلق" إن لم يحتوى النص المشفر على معلومات كافية لاستنتاج النص الصريح المناظر له مهما بلغ عدد النصوص المشفرة المتوفرة لدى المحلل. من المفروض في هذه الحالة ان لا يتمكن المحلل من فك تشفير الرسالة مهما توفر له من الوقت و القدرة الحاسوبية، حيث لا تتوفر المعلومات اللازمة لذلك.

لا توجد خوارزمية تشفير امنة بشكل مطلق، الا في حالة أساليب التشفير المعروفة باسم "مفتاح المرة الواحدة" (One-time pad). لذلك تصمم خوارزميات التشفير بناء على الاتي :

- ان تكون تكلفة تحليل الشفرة تفوق قيمة المعلومات المشفرة.
- ان يكون الزمن اللازم لتحليل الشفرة يفوق الفترة الزمنية المفيدة للمعلومات المشفرة.

ان توفرت هذه الشروط في أسلوب التشفير يكون امنا نسبيا ، و تكون الصعوبة في تقدير حجم المجهود اللازم لتحليل النص المشفر بنجاح.

2 – التشفير بالاستبدال (التبديل) :

التشفير بالاستبدال (التبديل) هو احد خوارزميات التشفير المتناظر (المفتاح السرى الواحد)، يعتمد هذا الأسلوب في التشفير على استبدال رمز بآخر. فإذا كانت الرموز الموجودة في النص الصريح عبارة عن أحرف أبجدية، فإننا نستبدل حرفًا بآخر، ويعاد ترتيبها دون تغيير فئة الحروف الصريحة.

على سبيل المثال، يمكننا استبدال الحرف (A) بالحرف (D)، والحرف (T) بالحرف (Z) .إذا كانت الرموز عبارة عن أرقام (من 0 إلى 9)، فيمكننا استبدال (3) بـ (7)، و (2) بـ (6). يمكن تصنيف التشفير بالاستبدال إما على أنها **أحادية الأبجدية** أو **متعددة الأبجدية**.

التشفير الأحادية الأبجدية

في التشفير بالاستبدال الأحادية الأبجدية، يتم دائمًا تغيير الحرف (أو الرمز) في النص الصريح إلى نفس الحرف (أو الرمز) المشفر بغض النظر عن موضعه في النص الصريح. على سبيل المثال، إذا غيرت خوارزمية التشفير الحرف (A) في النص الصريح إلى الحرف (D) في النص المشفر، فسيتم تغيير كل حرف (A) إلى الحرف (D) .وبعبارة أخرى، **في تشفير الاستبدال الأحادي الأبجدية، تكون العلاقة بين رمز في النص الصريح ورمز في النص المشفر دائمًا علاقة واحد لواحد.**

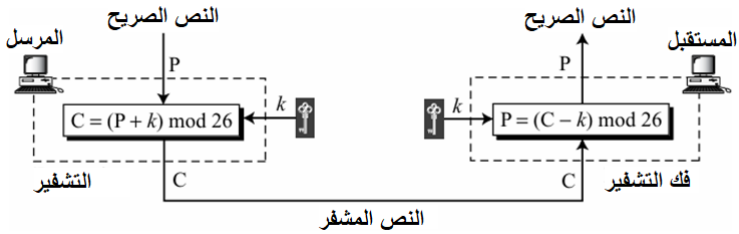
يعتبر **تشفير قيصر** من أبسط خوارزميات التشفير الأحادي الأبجدية. ويُطلق على هذا التشفير أحيانًا اسم **تشفير الازاحة** لكن مصطلح **تشفير الإضافة** يكشف بشكل أفضل عن طبيعته الرياضية. افترض أن النص الصريح يتكون من أحرف صغيرة (من (a) إلى (z))، وأن النص المشفر يتكون من أحرف كبيرة (من (A) إلى (Z). كي نتمكن من تطبيق عملية التشفير الرياضية على النص الصريح والنص المشفر، نقوم بتعيين قيم رقمية لكل حرف (أحرف صغيرة أو كبيرة)، كما هو موضح في الشكل.

النص الصريح	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
النص المشفر	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
القيمة	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

3 – التشفير بالاستبدال (التبديل) :

النص الصريح	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
النص المشفر	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
القيمة	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

في الشكل ، يتم تعيين عدد صحيح لكل حرف (أحرف صغيرة أو كبيرة) في مناظر لترتيبه الأبجدي (فئة الاحرف الإنجليزية - Z_{26}) .المفتاح السري بين طرفي الاتصال (التراسل) هو أيضًا عدد صحيح في (Z_{26} : من 0-25) ، تضيف خوارزمية التشفير المفتاح إلى حرف النص الصريح؛ تقوم خوارزمية فك التشفير بطرح المفتاح من حرف النص المشفر. تتم كافة العمليات في (فئة الاحرف الإنجليزية - Z_{26}) . ويبين الشكل التالي العملية. في **تشفير قيصر** ، يكون النص الصريح (P) والنص المشفر (C) والمفتاح السري (k) عدادًا صحيحا في فئة الاحرف الإنجليزية - Z_{26}.



مثال : استخدم تشفير قيصر بالمفتاح السرى (k) = **15** لتشفير الرسالة "**hello**". نطبق خوارزمية التشفير على النص الصريح، حرفًا بحرف، و النتيجة هي "**WTAAD**". لاحظ أن التشفير احادي الأبجدية لأنه تم تشفير حالتين من نفس حرف النص الصريح (**l**) الى بنفس الحرف المشفر (**A**).

النص الصريح (P): h ← 07	التشفير : (15+07) mod 26	النص المشفر (C): 22 ← W
النص الصريح : e ← 04	التشفير : (15+04) mod 26	النص المشفر : 19 ← T
النص الصريح : l ← 11	التشفير : (15+11) mod 26	النص المشفر : 00 ← A
النص الصريح : l ← 11	التشفير : (15+11) mod 26	النص المشفر : 00 ← A
النص الصريح : o ← 14	التشفير : (15+14) mod 26	النص المشفر : 03 ← D

3 – التشفير بالاستبدال (التبديل):

النص الصريح	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
النص المشفر	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
القيمة	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

التشفير المتعدد الأبجدية

في الاستبدال متعدد الابجدية ، قد يكون ظهور كل حرف له بديل مختلف. العلاقة بين حرف في النص الصريح وحرف في النص المشفر هي علاقة واحد لكثير. على سبيل المثال، يمكن تشفير (a) كـا (D) في بداية النص، ولكن كـا (N) في المنتصف. يتمتع التشفير متعددة الأبجدية بميزة إخفاء تكرار حروف في اللغة الأساسية. لا يستطيع الخصم (المهاجم) استخدام إحصائيات تكرار حرف واحد لكسر النص المشفر. لإنشاء تشفير متعدد الأبجدية، نحتاج إلى جعل كل حرف بالنص المشفر يعتمد على كل من حرف النص الصريح المطابق له وموضع حرف النص الصريح في الرسالة. وهذا يعني أن المفتاح يجب أن يكون عبارة عن مجموعة من المفاتيح الفرعية، حيث يعتمد كل مفتاح فرعي بطريقة ما على موضع حرف النص الصريح الذي يستخدم هذا المفتاح الفرعي للتشفير. بمعنى آخر، نحتاج إلى أن يكون لدينا دفق مفاتيح م = (م1، م2، م3، ...) حيث يتم استخدام مِن تشفير الحرف *ن* في النص الصريح لإنشاء الحرف *ن* في النص المشفر.

تشفير **بالمفتاح التلقائي** مثال على الاستبدال متعدد الابجدية ، في هذا التشفير، المفتاح عبارة عن دفق من المفاتيح الفرعية، حيث يتم استخدام كل مفتاح فرعي لتشفير الحرف المقابل في النص الصريح. المفتاح الفرعي الأول هو قيمة محددة مسبقًا تم الاتفاق عليها سرًا بين طرفي الاتصال. المفتاح الفرعي الثاني هو قيمة حرف الأول في النص الصريح (بين 0 و25). المفتاح الفرعي الثالث هو قيمة الحرف الثاني في النص الصريح. وما إلى ذلك. يشير اسم التشفير، **المفتاح التلقائي**، إلى أنه يتم إنشاء مفاتيح فرعية تلقائيًا من أحرف تشفير النص الصريح أثناء عملية التشفير.

$$P = P_1P_2P_3 \ldots \qquad C = C_1C_2C_3\ldots \qquad k = (k_1, P_1, P_2, \ldots)$$

Encryption: $C_i = (P_i + k_i) \bmod 26$ Decryption: $P_i = (C_i - k_i) \bmod 26$

النص الصريح	h	e	l	l	o
قيمة النص الصريح (P)	07	04	11	11	14
المفاتيح الفرعية (*K*)	12	07	04	11	11
قيمة النص المشفر (C)	19	11	15	22	25
النص المشفر	T	L	P	W	Z

مثال : استخدم التشفير **بالمفتاح التلقائي** بقيمة للمفتاح الأولي (k_1) = **12** لتشفير الرسالة **"hello"**. يتم التشفير حرفًا بحرف. يتم أولاً استبدال كل حرف في النص الصريح بقيمته الصحيحة كما هو موضح في الشكل. تتم إضافة المفتاح الفرعي الأول لإنشاء حرف النص المشفر الأول. يتم إنشاء بقية المفاتيح الفرعية أثناء قراءة أحرف النص الصريح. لاحظ أن التشفير متعدد الأبجدية لأن تكرارات الحرف (**l**) في النص الصريح يتم تشفيرها بشكل مختلف.

3 – التشفير بالنقل (الاحلال) :

W	H	A	T	W
A	S	T	H	E
W	E	A	T	H
E	R	L	I	K
E	O	N	F	R
I	D	A	Y	

W	H	A	T	W
A	S	T	H	E
W	E	A	T	H
E	R	L	I	K
E	O	N	F	R
I	D	A	Y	Z

W	A	W	E	E	I
H	S	E	R	O	D
A	T	A	L	N	A
T	H	T	I	F	Y
W	E	H	K	R	Z

التشفير بالنقل (التحويل) هو احد خوارزميات التشفير المتناظر (المفتاح السرى الواحد)، حيث لا يستبدل تشفير النقل رمزًا برمز آخر، بل يغير موقع الرموز. قد يظهر رمز في الموضع الأول من النص الصريح في الموضع العاشر من النص المشفر. قد يظهر رمز في الموضع الثامن في النص الصريح في الموضع الأول من النص المشفر. بمعنى آخر، يقوم تشفير النقل بإعادة ترتيب (الاحلال) الرموز.

في المثال التالي المفتاح هو رقم صغير. نستخدم رقم 5 كمفتاح. لتشفير رسالةٌ ما باستخدام هذا المفتاح، نكتب الرسالة في صفوف يتألف كل منها من خمسة أحرف، ثم نجري عملية التشفير من خلال كتابة أحرف العمود الأول أولا، ثم العمود الثاني ، وهكذا. إذا لم يساوِ طولَ الرسالة أحد أضعاف رقم 5 ، نُضيف عددا مناسبًا من حرف Z في النهاية قبل إجراء عملية التشفير. يمكن فهم عملية التشفير بسهولة بالغة من خلال مثال بسيط.

نشفِّر الرسالة (كيف كانت حالة الجو يوم الجمعة) (WHAT WAS THE WEATHER LIKE ON FRIDAY). بما أن المفتاح هو 5 ، تتضمن الخطوة الأولى إذن كتابة الرسالة في صفوف يتألف كل صف منها من خمسة أحرف، كالموضح بالجدول الأول.

بما أن طول الرسالة لا يساوي أحد أضعاف رقم 5 ،يجب إضافة حرف Z واحد لنحصل على النتيجة الموضحة بالجدول الثاني. نقرأ الآن كل عمود على التوالي لنحصل على النص المشفَّر التالي: **WAWEEIHSERODATALNATHTIFYWEHKRZ**

للحصول على مفتاح فك التشفير، نقسم طول الرسالة على المفتاح. في هذه الحالة، نقسم 30 على 5 لنحصل على 6 . تصبح خوارزمية فك التشفير الآن مماثلة لخوارزمية التشفير. لذا — على سبيل المثال — نكتب النص المشفَّر في صفوف تتألف من 6 أحرف لنحصل على النتيجة التي في الجدول الثالث.

يسهل الآن التحقق من أن قراءة كل عمود على التوالي سيفصح عن نص الرسالة الأصلية. يسهل كسر نوع الشفرات التبادلية المذكورة هنا. وبما أن المفتاح هو رقم يقسم طول النص المشفَّر، سوف يضطر الطرف المعترض إلى حساب طول النص المشفَّر وتجريب كل رقم يقبل القسمة عليه على التوالي.

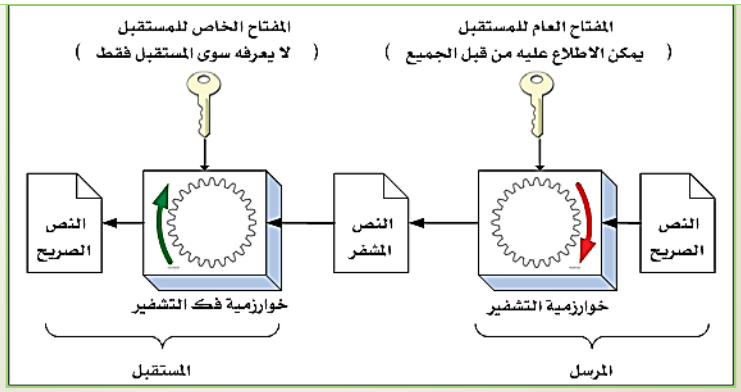
4 – التشفير بالمفتاح العام (غير التناظري)

يشير **"التشفير بالمفتاح العام"** او **"التشفير غير المتناظر"** إلى طرق التشفير التي تستخدم مفتاحين: أحدها للتشفير والآخر لفك التشفير، حيث لا يوجد مفتاح سري مشترك ما بين المرسل و المستقبل منذ البداية. و أنما يستخدم مفتاحان منفصلان، يستخدم احدهما للتشفير، و الاخر (وهو مرتبط بالأول) لفك التشفير. في هذا النوع من التشفير، ينشئ كل مستخدم زوجين من المفاتيح مرتبطين بعضهما ببعض (بطريقة رياضية معقدة لا تسمح بكشف اى منهما اذا عرف الاخر) احدهما **عام** ويمكن الاطلاع عليه من قبل كل المستخدمين، ويوزع المفتاح العام على نطاق واسع للسماح للمستخدمين بإرسال رسائل مشفرة لمالك المفتاح العام، و الاخر **خاص** بالمستخدم (سريا و خاص به) و يجب الا يطلع عليه الاخرون بتاتا، ويستخدم لفك التشفير. ومن الواضح أن صاحب المفتاح الخاص يحافظ علىُ مفتاحه بعناية. ولهذا السبب فإن مفتاح التشفير يسمى المفتاح العام، في حين أن مفتاح فك التشفير يسمى بالمفتاح الخاص. وتستخدم هذه التقنية اثنين من التطبيقات المختلفة - لنقل المعلومات والتوقيعات الرقمية.

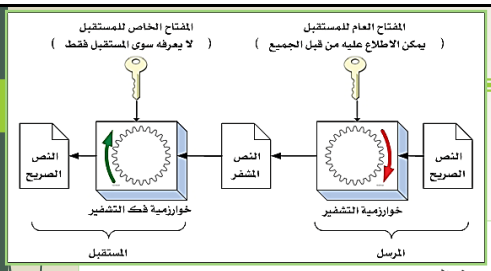
التشفير بالمفتاح العام يستنزف الموارد الحاسوبية ويتطلب قدرة معالجة حاسوبية تصل إلى ملايين المرات من تلك المطلوبة للتشفير بالمفتاح السري. وسيؤديُ الاستخدام المفرط للتشفير بالمفتاح العام بأسرع الأجهزة الحاسوبية المكتبية إلى التوقف شيئاً فشيئاً. ومن ثم فنحن في الواقع العملي انتقائيون للغاية فيا يخص استخدام التشفير بالمفتاح العام ونفضل استخدام التشفير بالمفتاح السري إلى أقصى حد ممكن. الاستخدام الرئيسي للتشفير بالمفتاح العام هو تبادل المفاتيح السرية في التشفير بالمفتاح السرى (التناظري).

4 – التشفير بالمفتاح العام : الالية

1. **عملية التشفير**: تشفر الرسالة الأصلية باستخدام خوارزمية التشفير والمفتاح العام للمستقبل للحصول على رسالة مشفرة. لاحظ أنه يمكن للمرسل الحصول على المفتاح العام للمستقبل؛ لأنه علني(مشاع) .
2. **عملية فك التشفير**: يتم فك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح الخاص (السري) للمستقبل؛ للحصول على الرسالة الأصلية، وبهذه الطريقة لن يستطيع أي شخص آخر فك تشفير الرسالة؛ لأنه لا يملك المفتاح الخاص للمستقبل.



4 – التشفير بالمفتاح العام : المكونات



1. **النص الصريح** : وهو النص أو الرسالة الأصلية المقروءة التي يتم إدخالها إلى خوارزمية التشفير.
2. **خوارزمية التشفير**: وهي الطريقة التي تشتمل على مجموعة الخطوات التي تنفذ على النص الصريح لإنتاج النص المشفر باستخدام المفتاح العام للمستقبل، وتكون مدخلات خوارزمية التشفير هي النص الصريح والمفتاح العام للمستقبل، ومخرجاتها هي النص المشفر.
3. **المفتاح العام** (Public Key) : وهو مفتاح عام (مشاع) بحيث يكون لكل طرف مفتاح عام يستخدم لتشفير أي رسالة ترسل اليه. يمكن لأى شخص الاطلاع على المفتاح العام واستخدامه في تشفير البيانات المرسلة إلى صاحب ذلك المفتاح العام، ويفك تشفير الرسالة المشفرة عن طريق المفتاح الخاص بالمستقبل (صاحب المفتاح العام الذى جري تشفير الرسالة به).
4. **المفتاح الخاص** (Private Key) : وهو عبارة عن مفتاح خاص سري، بحيث يكون لكل طرف مفتاح خاص سري خاص به يتم استخدامه لفك تشفير الرسائل الواردة إليه، ويكون هذا المفتاح مرتبطا بالمفتاح العام الخاص بالشخص نفسه.
5. **النص المشفر**: وهو عبارة عن الرسالة التي تنتجها خوارزمية التشفير من كل من النص الصريح والمفتاح العام للمرسل إليه.
6. **خوارزمية فك التشفير**: وهي مجموعة الخطوات التي يتم تنفيذها على النص المشفر لإنتاج النص الصريح، باستخدام المفتاح السري الخاص بالمستقبل. وتكون مدخلات خوارزمية فك الشفير هي النص المشفر والمفتاح السري الخاص بالمستقبل، ومخرجاتها هي النص الصريح.

4 – التشفير بالمفتاح العام : الآمان

للحصول على التشفير بالمفتاح العام آمن ، يجب تحقيق الشرطين:

1. استخدام خوارزمية قوية، بحيث يكون من غير الممكن حسابيا تحديد المفتاح السري الخاص بالمرسل إليه بمجرد معرفة هذه الخوارزمية و المفتاح العام (مفتاح التشفير).
2. يجب ان تبقى المفاتيح الخاصة سرية، و ان تنتج بطريقة عشوائية و بطول لا يقل عن 512 خانة ثنائية (بت) و ذلك للحد من هجوم البحث الشامل على المفتاح رغم انه قد يجعل ذلك النظام بطيئا.

لذلك يوجد نظام متكامل للتشفير بالمفتاح العام يسمى "البنية التحتية للمفاتيح العامة" – (PKI)، ويستخدم كأسلوب رئيس لتحقيق السرية للمشتركين . اشهر نظم التشفير بالمفتاح العام (غير المتناظر) هي:

- نظام ار اس ايه (RSA) .
- نظام (AES)
- نظام المنحنى البيضاوي (ECC) .

5 – التشفير بالمفتاح العام / التشفير بالمفتاح السري : مقارنة

التّشفير المتناظر	التّشفير غير المتناظر
١. يتم استخدام نفس المفتاح عند المرسل والمستقبل ونفس الخوارزميّة لكل من عمليّة التّشفير وفك التّشفير.	١. يتم استخدام نفس الخوارزميّة للتشفير وفك التّشفير.
٢. يجب إن يتم توزيع المفتاح السِّريّ بطريقة آمنة.	٢. يستخدم زوج من المفاتيح أحدهما عام يطلع عليه الآخرون، والآخر سري خاص بكل مستخدم (ليس نفس المفتاح عند المرسل والمستقبل)
٣. يحتاج إلى عمليّة توزيع آمنة للمفاتيح السِّريّة.	٣. لا يحتاج إلى عمليّة توزيع المفاتيح.

6 – التشفير بالمفتاح العام / التشفير بالمفتاح السري : مستوى السرية

مستوى السرية : يكون للخوارزمية مستوى سرية (ن) خانة ثنائية (بت) اذا كان عدد خطوات افضل هجوم معروف عليها هو ($2^{ن}$) خطوة. وهذا يتفق مع كون قوة خوارزمية التشفير المتناظر تساوى طول مفتاح التشفير المستخدم. يوضح الجدول التالي **طول مفتاح التشفير** اللازم لبعض **مستويات السرية** لبعض **خوارزميات التشفير** بنوعيه: المتناظر و غير المتناظر.

نوع التشفير	الخوارزمية	مستوى السرية			
		80	128	192	256
السري	AES	80	128	192	256
العام	RSA	1024	3072	7680	15360
	ECC	160	256	384	512

من الجدول، يكمن القول إنه يمكن الحصول على خوارزمية تشفير بقوة (80) خانة ثنائية (بت)، (اى تحتاج الى (2^{80}) خطوة لكسر تشفيرها)، باستخدام خوارزمية تشفير متناظر بمفتاح تشفير طوله (80) خانة ثنائية - بت، او باستخدام خوارزمية التشفير غير المتناظر (RSA) بطول مفتاح تشفير (1024) خانة ثنائية ، او باستخدام خوارزمية التشفير بالمنحنى البيضاوى (ECC) بطول مفتاح تشفير (160) خانة ثنائية. وبصفة عامة فإن طول مفتاح التشفير يزداد بازدياد مستوى السرية المطلوب لأى لخوارزمية، ومن الملاحظ من الجدول السابق انه يمكن الحصول على مستوى السرية لخوارزمية التشفير بالمنحنى البيضاوى (ECC) نفسه باستخدام مفتاح تشفير أقل بكثير من طول مفتاح التشفير لخوارزمية التشفير غير المتناظر (RSA) لمستوى السرية نفسه، أو باستخدام مفتاح تشفير بضعف طول مفتاح التشفير المتناظر، لمستوى السرية نفسه كذلك.

7 – التشفير الكتلي

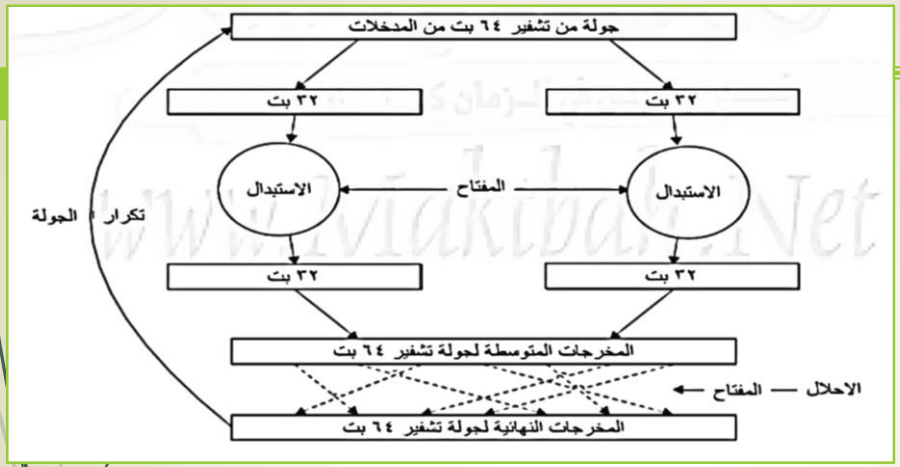
يعالج **التشفير الكتلي** كتلة كاملة (مجموعة من الاحرف او الأرقام او الرموز ....) من النص الصريح مرة واحدة، مثل إحلال رمز كبير قد يزيد حجمه عن 64 ثنائية (بت). يتطلب تشفير الكتلة توفر المعلومات قبل البدء في عملية التشفير. أساليب التشفير الكتلي المعتمدة على المفتاح السري تعتبر من اكثر نظم التشفير أهمية و استخداما في كثيرا من التطبيقات، كما لا يوجد تشفير كتلي مناسب لجميع التطبيقات و ذلك لاختلاف متطلبات التشفير من تطبيق الى آخر.

بشكل عام يستخدم تشفير الكتلي مزيجاً من النشاطين التالين: الاستبدال والنقل (الإحلال). وفي سياق التشفير بالمفتاح السري، يحدد الاستبدال مخرجات 1000 ثنائية لكل 1000 مدخلات. أما النقل فيحدد مكان المخرجات لكل 1000 ثنائية من المدخلات. ويعد النقل حالة خاصة من الاستبدال لأن كل ثنائية من المدخلات تستبدل ثنائية محدد من المخرجات. ويوضح الشكل العملية العامة للتشفير الكتلي.

ويمثل الشكل والمعتمد على تقنية معيار تشفير البيانات (DES)، العملية العامة لتقنيات التشفير بالمفتاح السري حيث يتم داخل كل كتلة تقسيم البيانات إلى قسمين. ثم تتم إجراء عملية الاستبدال لجميع الثنائيات في كلا القسمين. ويتم تمرير كلا القسمين على وحدة الإحلال والتي تقوم بخلط جميع الثنائيات في الكتلة. وتتكرر هذه العملية حتى يتم تشفير المدخلات بشكل مرض.

في هذا النوع من التشفير يُجزّأ النص الصريح الى كتل متساوية الحجم ، ثم تشفر كل كتلة باستخدام نفس مفتاح التشفير. يتم استخدام نفس مفتاح التشفير مع كل كتلة من كتل النص الصريح، ولا يشترط أن يكون حجمه (طوله) يساوى حجم كتلة النص الصريح. ويختلف حجم الكتلة، وطول مفتاح التشفير من خوارزمية الى أخرى. ففي نظام التشفير بمعيار تشفير البيانات (DES)، يكون حجم الكتلة (64) خانة ثنائية و طول مفتاح التشفير (56) خانة ثنائية، اما في نظام التشفير القياسي (AES) يكون حجم الكتلة (128) خانة ثنائية و طول مفتاح التشفير (128،192،256) خانة ثنائية ، والمفتاح (128) هو الأكثر انتشارا.

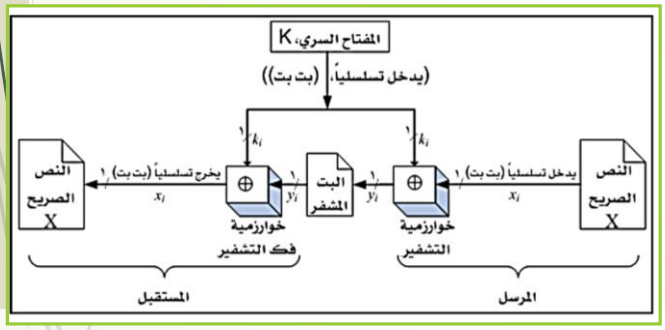
7 – التشفير الكتلي



يتم تكرار عملية الاستبدال / النقل عدة مرات لضمان أن التغيرات في المدخلات تم توزيعها على جميع الثنائيات في المخرجات. وفي الشكل، سيؤثر التغيير في ثنائية واحدة من المدخلات على 32 ثنائية من 64 ثنائية في المخرجات في الجولة الواحدة (إما النصف الأيمن أو النصف الأيسر، يليها تغييرات في 32 ثنائيا المقابلة من المخرجات الأخرة للجولة) . وهذا ليس مرضياً. للحصول على تشفير جيد، يجب أن يؤثر أي تغيير في ثنائي واحدة من المدخلات على جميع 64 ثنائي في المخرجات على حد سواء. وهذا سيجعل التشفير صعب الاختراق على المتسلل. ولتحقيق ذلك يتم تكرار الجولات حتى تتأثر جميع الثنائيات بأي تغيير في المدخلات حتى لو كان بسيطاً. معيار تشفير البيانات (DES) يستخدم 16 جولة تكرار. ومعيار التشفير المتقدم (AES) يستخدم 10 – 14 جولة تكرار اعتماداً على حجم المفتاح.

8 – التشفير التدفقي

في هذا النوع من التشفير يتم تشفر كل خانة ثنائية (Bit) من النص الصريح بشكل منفرد، بحيث يؤخذ النص الصريح تسلسليا خانة بخانة حتى نهايته. ويستخدم في هذه الحالة مفتاح تشفير تسلسلي أيضا (تدفق مفتاحي عشوائي)، بحيث تستخدم كل خانة منه لتشفير خانة واحدة من النص الصريح وإنتاج خانة واحدة من النص المشفر، و يتطلب تأمين التشفير التدفقي عدم إعادة استخدام تدفق المفتاح حتي لا يتم تحليل النص المشفر بسهولة كما هو موضح بالشكل التالي:



- **عمليّة التّشفير:** تكون بتطبيق العمليّة المنطقيّة «أو الحصريّة»(XOR) (أو الجمع القياسي للقياس ٢ (Modulo 2) على بت النّص الصريح، والبت الذي يقابله من مفتاح التّشفير؛ لإنتاج بتّ واحد من النّص المشفّر، وفق المعادلة الرياضيّة الآتية:

$$y_i = x_i \oplus k_i$$

- **عمليّة فكّ التّشفير:** تتم بتطبيق العمليّة المنطقيّة «أو الحصريّة»(XOR) على بت النّص المشفّر، والبت الذي يقابلة من مفتاح التّشفير؛ لإنتاج بت واحد من النّص الصريح، وفق المعادلة الرياضيّة الآتية:

$$x_i = y_i \oplus k_i$$

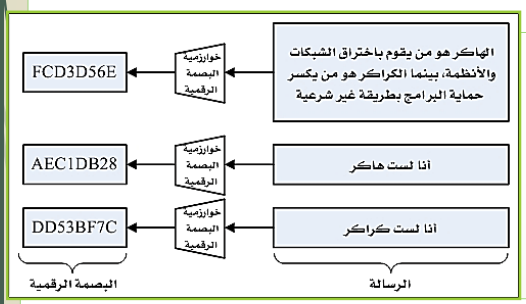
التشفير التدفقي يتميز بالميزات التالية:

- استخدام الخوارزمية نفسها (الدالة) لعمليتي التشفير و فك التشفير، وهى في هذه الحالة العملية المنطقية "أو الحصرية" (XOR) (الجمع القياسي للقياس 2).
- سهولة بناء نظام تشفير سريع و صغير الحجم، سواء كان نظام برمجيا او نظاما ماديا. و يعود ذلك (السرعة و صغر الحجم) الى كونه نظام تشفير يتعامل مع خانة ثنائية واحدة في الوقت الواحد.
- إمكانية استخدام مفتاح تشفير تدفقي طويل جدا، الى درجة انه يمكن ان يكون طوله يساوى طول الرسالة المراد تشفيرها، وهو ما يعرف بنظام التشفير "مفتاح المرة الواحدة"، والذى يستخدم مفتاح تشفير عشوائي يختلف في كل عملية تشفير.

9 – البصمة الرقمية : دوال الاختزال (القيمة المركزة)

تشير دوال الاختزال إلى طرق التشفير التي لا تستخدم مفاتيح. وتسمى هذه الدوال أيضاً تحويلات الاتجاه الواحد لأنه لا توجد وسيلة لاسترداد الرسالة المشفرة باستخدام دالة الاختزال. لماذا نهتم بتقنية تشفير إذا كانت لا تسمح أبداً بقراءة البيانات مرة أخرى؟ هذه التقنية في الواقع مفيدة جداً.

تتمثل الفكرة الأساسية لدوال الاختزال في أن قيمة التشفير في القيمة المركزة الناتجة تمثل صورة مختصرة للرسالة الأصلية. وللقيمة الناتجة عن اختصار الرسالة الأصلية أسماء عدة ؛ مثل «البصمة الرقمية»، و«مختصر الرسالة»، وبالطبع «قيمة التشفير المحور» و "القيمة المركزة". وتضمن عملية التشفير هذه عددا من التطبيقات؛ منها تحقيق تكامل البيانات واستخدامها في عملية التصديق الرقمي.



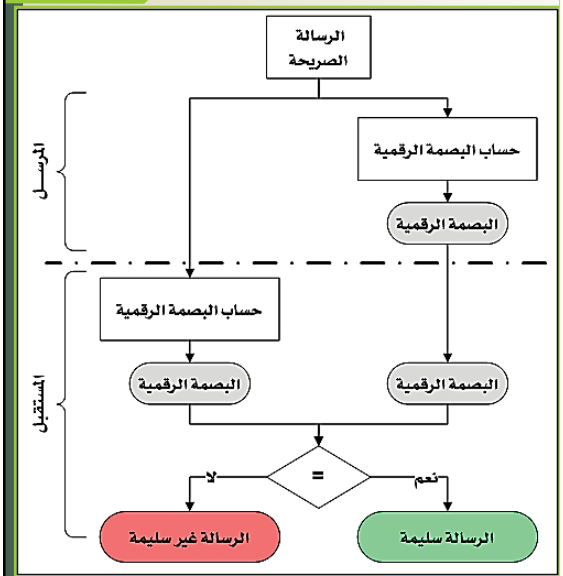
بوجه عام، تقبل دوال الاختزال مَدخلات بأي طول وتُنتِج مَخرجات ثابتة الطول. إذا أنتج مدخلان المخرج نفسه، نطلق على ذلك «صدام». ويعتبر وجود صدام مسألة حتمية. من هنا، إذا أردنا تحديد رسالة ما تحديدا دقيقًا من خلال بصمتها الرقمية، يجب انتقاء دالة الاختزال جيدا لضمان استحالة اكتشاف حالات الصدام حتى في حال وجودها. يترتب على ذلك عدد من النتائج، تتمثل إحداها في ضرورة ارتفاع عددً قيم البصمات الرقمية الممكنة. لبيان السبب في ذلك، نذكر مثالاً بسيطا للغاية. إذا كانت هناك ثمانية قيم محتملة فقط للبصمة الرقمية، فسيكون هناك احتمال نسبته 12.5٪ في أن يكون لرسالتين اعتباطيتين نفس القيمة. بالإضافة إلى ذلك، يكون من المضمون اشتمال أي مجموعة تتألف من تسع رسائل أو أكثر على حالة صدام واحدة على الأقل.

تستخدم دوال الاختزال لتحويل المدخلات إلى مخرجات ذات طول ثابت (البصمة الرقمية). ولهذا التحويل خاصيتان:

1. كل عنصر من المدخلات يقابله عنصر فريد من المخرجات،
2. ومن المستحيل تخمين أحد المدخلات بناء على المخرجات المحددة.

ويمكن ملاحظة أن جميع المدخلات لها مخرجات فريدة (بصمة) وهذا هو سبب تسمية هذا التحويل بالاختزال . وعند تحديد مخرجات الاختزال فإنه من المستحيل معرفة أن عنصراً معيناً من المدخلات قد أدى إلى المخرجات المحددة، وهى بصمة مختلفة لكل رسالة لكن جميع البصمات طولها واحد و ثابت.

9 – البصمة الرقمية : دوال الاختزال (القيمة المركزة)



بما ان البصمة الرقمية تظهر بوضوح اى تغيير –ولو كان بسيطا جدا- على الرسالة الاصلية؛ فانه يمكن من خلال ذلك كشف اى تعديل او حذف او إضافة على الرسالة الاصلية. وتتخلص طريقة استخدام البصمة الرقمية للتحقق من سلامة محتوى الرسالة فيما يلى (حسب الشكل) :

1. يحسب المرسل البصمة الرقمية للرسالة باستخدام احدى خوارزميات البصمة الرقمية.
2. يرسل المرسل الرسالة الاصلية متبوعة بالبصمة الرقمية.
3. عند استلام الرسالة من قبل المستقبل يعيد حساب البصمة الرقمية للرسالة عند استلامها.
4. يقارن المستقبل البصمة الرقمية التي حصل عليها في الخطوة السابقة (3) مع البصمة الرقمية التي استلمها مع الرسالة، فاذا تطابقت القيمتان، فهذا دليل على ان الرسالة سليمة و لم يطرأ عليها اى تغيير، اما اذا لم تتطابق فهذا دليل على ان الرسالة غير سليمة، وانه طرأ عليها تغيير ما.

دوال الاختزال الأكثر استخداماً وشيوعاً هما دالة (MD5) ودالة (SHA-2). وقد استخدمت دالة (MD5) عالمياً منذ تطويرها في عام 1991، ولكن تم اكتشاف عيوب في الخوارزمية، ومن ثم فإن استخدامها في تطبيقات التشفير لم يلق تشجيعاً منذ 2008 ومع ذلك لا تزال تستخدم في التطبيقات المنخفضة المخاطر. اما الدالة (SHA-2) فقد تم إصدارها في عام 2001، ويرمز الرقم (2) إلى الإصدار الثاني منها، وعلى الرغم من عدم وجود ثغرات أمنية معروفة لهذه الخوارزمية إلا أن الإصدار التالي لهذه الدالة (SHA-3) كان في عام 2012، وذلك للبقاء على استعداد في حال حدوث هجوم ضد دالة (SHA-2).

10 – التوقيع الرقمي

الاستخدام الثاني للتشفير بالمفتاح العام تأتي من العلاقة الفريدة بن المفتاح العام والمفتاح الخاص المرتبط به حيث أن تلك المفاتيح توجد في أزواج، حيث أن المعلومات المشفرة باستخدام المفتاح العام يمكن فك تشفرها بواسطة المفتاح الخاص المرتبط بذلك المفتاح العام. ويمكن لهذه العملية أن تعمل أيضاً في الاتجاه المعاكس. المعلومات المشفرة باستخدام المفتاح الخاص يمكن فك تشفيرها بواسطة المفتاح العام المرتبط بذلك المفتاح الخاص. ويتم استخدام هذه الميزة في مجال أمن المعلومات إنشاء التوقيعات الرقمية. وتعرف التوقيعات الرقمية بأنها تحويلات مشفرة من البيانات تسمح لمستقبل هذه البيانات بإثبات مصدر البيانات (عدم التنصل) وتكاملها.

يمكن تصنيف **التوقيع الرقمي** الى مجموعتين : التوقيعات الرقمية المباشرة ، و التوقيعات الرقمية التحكمية. ويمكن تلخيص خواص التوقيع الرقمي في الاتى :

- ان يعتمد التوقيع الرقمي على الرسالة الموقعة.
- ان يستخدم معلومات المرسل الفريدة لمنع التزوير و الانكار.
- ان يكون انتاج التوقيع الرقمي وتمييزه والتحقق منه سهلا.
- ان يكون حساب التوقيع الرقمي صعب على المزورين لتوقيع الرسائل الجديدة او رسالة محددة.
- ان يمكن حفظه بأمان.

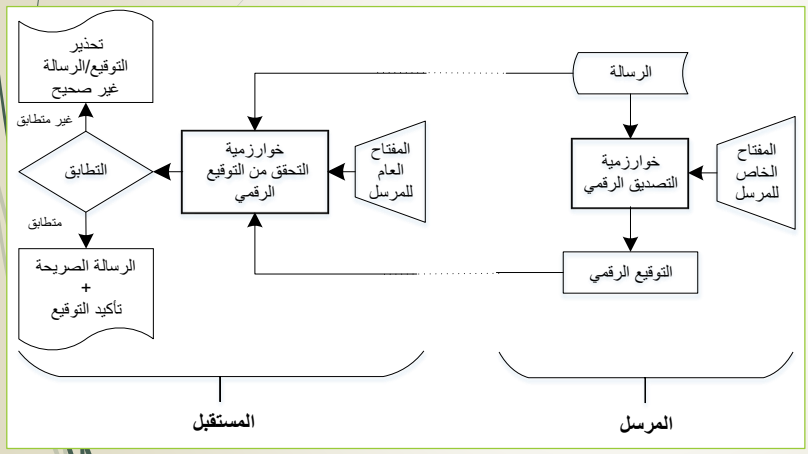
تتطلب التوقيعات الرقمية المباشرة التطبيق المباشر لنظام التشفير بالمفتاح العام بين اطراف الاتصال (المرسل و المستقبل). يفترض ان المستقبل على دراية بمفتاح المرسل العام. يمكن إنشاء التوقيع الرقمي بتشفير كل الرسالة باستخدام مفتاح المرسل الخاص، ونتحصل على السرية بتشفير الرسالة كاملا بالإضافة الى التوقيع باستخدام أسلوب المفتاح العام او أسلوب المفتاح السري. ويفك التشفير باستخدام مفتاح المستقبل العام . من المهم ان نقوم أولا بتوقيع الرسالة، وذلك للسماح في حالة النزاعات لطرف ثالث بالاطلاع على الرسالة و التوقيع. يعتمد امن أسلوب التوقيع المباشر على امن مفتاح المرسل الخاص، وفى حالة فقده او سرقته يعرض التوقيع للتزوير.

المشاكل المرتبطة بالتوقيعات الرقمية المباشرة يمكن حلها باستخدام التوقيعات الرقمية التحكمية و بترتيبات مختلفة. يتطلب هذا الأسلوب وجود حكم (طرف ثالث) تتمثل مهمته في التصديق (مصادقة رسمية) على الرسالة الموقعة و يؤرخها ثم يرسلها الى المستلم. يقوم الحكم بدور حساس و حاسم في هذه الطريقة، ويجب ان تكون لدى جميع الأطراف ثقة بان آلية التحكيم تعمل كما ينبغي. يتحقق التوقيع الرقمي التحكمي باستخدام نظام المفتاح العام و يمكن للحكم الاطلاع او عدم الاطلاع على الرسالة.

10 – التوقيع الرقمي

التوقيع الرقمي يتكون من عمليتين أساسيتين (كما هو موضح بالشكل)، وهما :

- التوقيع : وهو عملية اجراء (انتاج) التصديق الرقمي، و مدخلاتها هي: الرسالة و المفتاح الخاص للمرسل (الموقع)، و نتيجتها التوقيع الرقمي، ويرسل مرفقا مع الرسالة.
- التحقق من صحة التوقيع : وهو عملية التحقق من ان التوقيع تم من الشخص المعنى على الرسالة، و مدخلاتها هي: الرسالة و المفتاح العام للمرسل (الموقع)، ونتيجتها احدى الحالتين: مطابق او غير مطابق.



10 – آلية التوقيع الرقمي : التوقيع ، التحقق ، الاعتراف

عملية التوقيع :

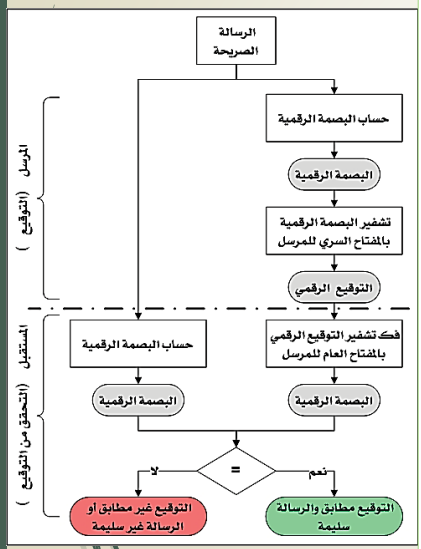
1. يتم حساب البصمة الرقمية للرسالة المراد توقيعها.
2. يتم تشفير هذه البصمة الرقمية باستخدام المفتاح السري للمرسل (الموقّع) لإنتاج "التوقيع الرقمي" للرسالة.
3. يتم ارسالها مع الرسالة الصريحة الى المرسل اليه.

عملية التحقق من صحة التوقيع :

1. يفك المستقبل تشفير "التوقيع الرقمي" باستخدام المفتاح العام للمرسل، لتظهر البصمة الرقمية للرسالة الاصلية في صورتها الصريحة (غير المشفرة).
2. يحسب المستقبل البصمة الرقمية للرسالة الصريحة (المستقبل استلم الرسالة الصريحة مع التوقيع الرقمي) لإنتاج البصمة الرقمية للرسالة من جديد، لكن من الطرف الاخر لإجراء عملية مقارنة.
3. يقارن المستقبل البصمة الرقمية التي حسبها سابقا مع البصمة الرقمية التي استلمها مع الرسالة الاصلية. فاذا تطابقت هاتان القيمتان، فان ذلك يكون كافيا لأثبات ان هذه الرسالة مصدرها هو المرسل فعلا، حيث انه تم تشفيرها بواسطة مفتاحه الخاص، وانها سليمة لم يطرأ عليها أي تعديل، حيث انتج النص المستلم نفس البصمة الرقمية، اما اذا لم تتطابق فهذا يعنى ان التصديق الرقمي غير صحيح، او ان الرسالة غير سليمة او تم تعديلها.

يحقق التوقيع الرقمي الشروط اللازم توافرها للاعتراف به على النحو التالي :

1. يتم التوقيع الرقمي باستخدام المفتاح الخاص للمرسل، والذى لا يعرفه ولا يملكه احد غيره، بمعنى انه هو الذى وقع الوثيقة و انه ملتزم بما ورد فيها (عدم الانكار).
2. التوقيع الرقمي مستنتج من النص الأصلي (الصريح)؛ لأنه تم التشفير بالبصمة الرقمية للرسالة الاصلية، وهذا يعنى :
   I. ان الوثيقة لم يتم تغييرها بعد استخراج التوقيع الرقمي.
   II. انه لا يمكن نسخ التوقيع الرقمي او نقله الى رسالة أخرى، و الا فانه بعد فك تشفير لن ينتج "البصمة الرقمية" نفسها.



10 – التوقيع الرقمي : تشفير الرسالة مع التوقيع الرقمي

عندما ترسل سعاد رسالة إلى احمد فإنه يمكنها أيضاً أن ترسل قيمة مركزة من الرسالة مشفرة باستخدام المفتاح الخاص بها. وبإمكان احمد أن يحاول فك شفرة هذه القيمة، فإذا كانت القيمة التي تم فك شفرتها توافق المعلومات المرسلة بالرسالة فإن احمد على يقين بأن سعاد هي التي أرسلت الرسالة وأن الرسالة لم يتم تعديلها وهي في طريق الإرسال. وتظهر هذه العملية في الشكل. في كل حالة نقل المعلومات نستخدم مفاتيح المستقبل، وفى حالة التوقيعات نستخدم مفاتيح المرسل. لنقل المعلومات يستخدم المفتاح العام للتشفير، ولكن التوقيعات الرقمية تستخدم المفتاح الخاص للتشفير (الجدول التالي يلخص ذلك). الامر الذي يجب أن تذكره بخصوص التشفير بالمفتاح العام أن المستخدم يمكنه الوصول إلى مفتاح خاص واحد وهو المفتاح الذي يملكه، ولكن الجميع لديه حق الوصول إلى جميع المفاتيح العامة.

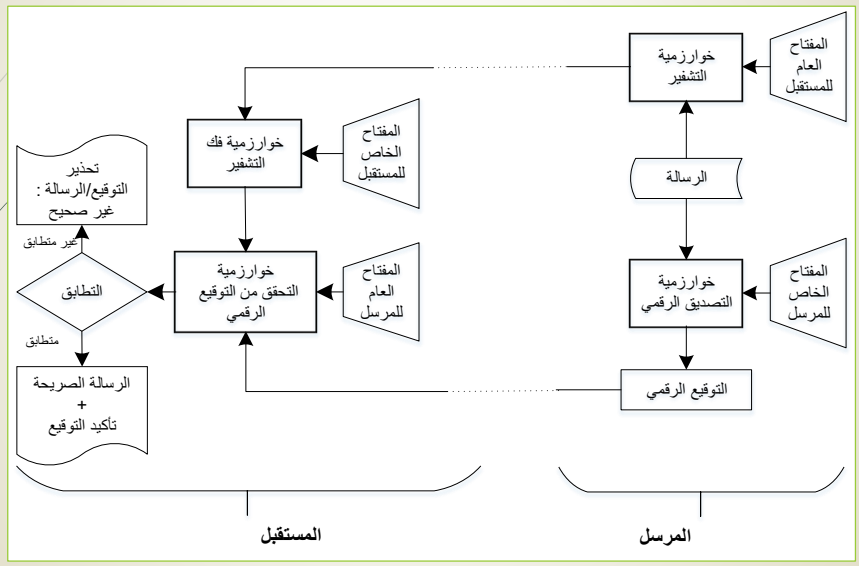
وعند نقل المعلومات، نرغب في التأكد من أن تلك المعلومات لا يمكن قراءتها من قبل الآخرين أثناء الإرسال. وأفضل طريقة لتحقيق ذلك هي تشفير المعلومات بطريقة يستطيع المِستقبل فقط من خلالها فك شفرة المعلومات.

كما نعرف أن المستقبل يملك فقط المفتاح الخاص به. كما نعلم أيضاً أننا إذا قمنا ُ بتشفير بعض المعلومات باستخدام المفتاح العام للمستقبْل، فإن المِستقبل فقط سيكون قادراً على فك شفرة المعلومات باستخدام مفتاحه الخاص. ولكن أي شخص في العالم يمكنه الحصول على المفتاح العام لأي مستخدم. لذلك سوف تشفر ُ المعلومات باستخدام المفتاح العام للمستقبل ومن ثم إرسالها. وعندها سيكون المستقبل فقط قادراً على قراءة المعلومات.

عند التوقيع على الرسائل فإن الخصوصية ليست مصدراً للقلق. على سبيل المثال، يرغب احمد أن يكون مقتنعاً بأن سعاد هي بالفعل من قامت بإرسال الرسالة ، كيف يمكن لسعاد القيام بذلك؟ حسناً ً، كل من سعاد واحمد يعلم أن فقط سعاد تملك المفتاح الخاص بها. إذا كانت سعاد تستطيع إقناع احمد بطريقة أو بأخرى بأنها بالفعل تمتلك هذا المفتاح، فإن احمد سوف يقتنع. ولحسن الحظ لدينا طريقة للقيام بذلك. إذا قامت سعاد بتشفير بعض المعلومات باستخدام مفتاحها الخاص، فإن أي شخص في العالم يستطيع فك شفرة المعلومات باستخدام مفتاحها العام. وفي الواقع فإن احمد يقوم بذلك بالضبط. وإذا نجح فإنه سيكون مقتنعا بأن سعاد تملك المفتاح الخاص الذي يفترض أن يكون لديها. لأنه لا أحد في العام يجب أن يكون لديه المفتاح الخاص بسعاد، فإن الرسالة يجب أن تكون قد ارسلت من سعاد ومن ثم فإن المفتاح العام يعمل بمثابة توقيع رقمي.

الطريقة التي يتم بها استخدام التوقيعات الرقمية في الواقع العملي تعطي ميزة إضافية. ما الرسالة التي يجب أن تقوم سعاد بتشفيرها وإرسالها إلى احمد وإقناعه بهويتها؟ نحن نقوم بتشفير الرسالة، وبهذه الطريقة إذا استطاع احمد أن يفك الشفرة بنجاح سيقتنع بأن الرسالة ليست فقط أرسلت من سعاد ، بل سيتأكد أيضاً ً أن الرسالة لم يتم تعديلها اثناء الإرسال.

10 – التوقيع الرقمي : تشفير الرسالة مع التوقيع الرقمي



التشفير: مقارنة الاستخدام

مقارنة بين أنواع التشفير

نوع التشفير	المفاتيح	التطبيقات
دوال الاختزال / (البصمة الرقمية)	0	حماية كلمات المرور، تحقيق نزاهة المعلومات.
التشفير بالمفتاح السري	1	حفظ و نقل آمن للمعلومات.
التشفير بالمفتاح العام	2	ضمان الآمن لكل من تبادل المفاتيح، المصادقة، والتوقيعات الرقمية.

مقارنة لتطبيقات التشفير بالمفتاح العام

	نقل المعلومات	التوقيع الرقمي
مالك المفتاح	المستقبل	المرسل
نوع مفتاح التشفير	عام	خاص

11 – التورية (Steganography) :

النص المخفي في الرسالة ؟

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16t proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

A Puzzle for Inspector Morse
(From The Silent World of Nicholas Quinn, by Colin Dexter)

11 – التورية: (Steganography)

قد يتم إخفاء المعلومات (النص الصريح) باستخدام احدى طريقتين؛ **التورية** وبهذا الطرق يتم اخفاء وجود المعلومات بطريقة لا يشك أحد في وجودها، في حين أن طرق **التشفير** تجعل المعلومات غير مفهومة للغرباء من خلال اجراء تحويلات مختلفة على نص الرسالة.

إن ابسط شكل لعلم الإخفاء ، ولكنه يستغرق وقتًا طويلاً في بنائه ، هو الاسلوب الذي تخفي به ترتيب كلمات أو حروف الرسالة الحقيقية داخل نص يبدو أنه غير ضار. على سبيل المثال ، يوضح تسلسل الأحرف الأولى من كل كلمة في الرسالة المرسلة (المعلنة) الرسالة المخفية. يوضح الشكل التالي مثالاً تُستخدم فيه مجموعة فرعية من كلمات الرسالة المرسلة لنقل الرسالة المخفية. معرفة ما إذا كان يمكنك فك هذا ؛ ليس من الصعب جدا.

تم استخدام تقنيات أخرى مختلفة تاريخيا ؛ بعض الأمثلة هي التالية:

- تعليم الحروف: يتم الكتابة فوق الحروف المحددة من النص المطبوع أو المكتوب على الآلة الكاتبة بالقلم الرصاص. عادة ما تكون العلامات غير مرئية إلا إذا تم إمساك الورق بزاوية للضوء الساطع.
- الحبر غير المرئي: يمكن استخدام عدد من المواد للكتابة ولكن لا تترك أثرًا مرئيًا حتى يتم تطبيق الحرارة أو بعض المواد الكيميائية على الورق.
- ثقوب الدبوس: ثقوب الدبوس الصغيرة على الحروف المختارة غير مرئية عادة ما لم يتم رفع الورق أمام الضوء.
- شريط تصحيح الآلة الكاتبة: يستخدم بين الأسطر المطبوعة بشريط أسود ، ولا تظهر نتائج الكتابة بشريط التصحيح إلا تحت ضوء قوي.

11 – التورية: (Steganography)

مكنت تقنيات الحواسيب الحديثة من تضمين نصوص مخفية بكفاءة وسهولة بحيث تقوم الحواسيب بتشفير الرسالة وإخفائها داخل ملف آخر. ويمكن تعريف التورية بأنها "فن إخفاء وجود المعلومات داخل ملفات تبدو غير ضارة" حيث أن "الرسالة المشفرة قد تثير الشكوك بينما لا تفعل الرسالة المخفية ذلك". وبالتالي، فإن الهدف هو إخفاء حقيقة وجود الرسالة في المقام الأول، بحيث ان أي شخص يعترض ويشاهد الملف (صورة أو مستند أو بريد إلكتروني وما إلى ذلك) لا دراية له بالبيانات المخفية. كما يمكن تعريف البيانات المضمنة بأنها المعلومات التي سيتم إخفاؤها في ملف ناقل (الغلاف) أصلي بريء مثل صورة أو صوت أو نص أو فيديو، تسمى العملية نفسها التورية، ويشكل الملف الناقل (الغلاف) والبيانات المضمنة معًا بيانات التضمين.

كما ذكرنا سابقًا، تهدف كل من التورية والتشفير إلى إخفاء المعلومات. تخفي التورية وجود الرسالة، ويجعل التشفير الرسالة مستحيلة الفهم بالنسبة للغرباء، وكثيرًا ما يتم استخدام كليهما معًا. في حين يمكن التعرف بسهولة على الرسائل المشفرة في حد ذاتها من خلال مظهرها العشوائي وغير المفهوم، تبدو رسائل المخفية بالتورية طبيعية للوهلة الأولى. ويمكن أن يوفر الاستخدام المشترك للتورية والتشفير لمرسل الرسالة مستويين من الحماية بشكل فعال.

هناك تقنية أخرى ذات صلة وهي وضع العلامات المائية، حيث يتم تمييز الملفات الرقمية بشكل مرئي أو غير مرئي بمعلومات مضمنة. في عملية العلامات المائية، لا يكون النص المضمن في النص الصريح بل في الناقل (الوعاء) نفسه. تعمل العلامة المائية فقط على تحديد الناقل (الوعاء) بشكل فريد. يمكن أن يكون هذا واضحًا كرادع للنسخ الرقمي، أو مخفيًا كدليل على الملكية والأصل. تقوم شركات البث التلفزيوني بشكل روتيني بتضمين علامة مائية مرئية في برامجها، وتستخدم أنظمة حماية حقوق النشر علامات مائية غير مرئية. يشير هذا إلى الحاجة إلى عدم الفصل بين العلامة المائية والناقل (الوعاء) ، حيث أن إزالة العلامة المائية (المرئية أو غير المرئية) تدمر إمكانية ردع النسخ الغير شرعي وإثبات الملكية.

11 – التورية: (Steganography)

هناك مشكلة خاصة لكل من التورية والعلامة المائية وهي ان تحويل الملفات الرقمية إلى تنسيقات مختلفة أو بمستويات ضغط مختلفة يمكن أن يؤثر كلاهما على المعلومات المضمنة، ويجب أن تكون التقنية قوية ضد هذا النوع من الهجومات وتعديل الإشارة. على سبيل المثال، خوارزميات الضغط بدون فاقد فقط (مثل GIF، وليس JPEG) مناسبة للإخفاء التضليلي، ذلك لأن البيانات المضمنة (المخفية) قد تتغير. قد تقوم بروتوكولات نقل معينة أيضًا بضغط الإشارة بطرق قد تعرض قدرة المستقبل على اكتشاف البيانات المضمنة (المخفية) للخطر. أخيرًا، في حين أن المحتوى المخفي (المضمن) قد يفقد أهميته عندما تصبح المعلومات قديمة أو باهتة، فإن العلامات المائية تحتفظ بأهميتها إلى أجل غير مسمى. يتضمن الجدول التالي مقارنة موجزة بين التقنيات الثلاث.

الجدول : مقارنة بين التورية (التخفي) والتشفير والعلامات المائية

التقنية	الغرض	التعليقات
التورية (الاخفاء)	إخفاء وجود المحتوى الرقمي (الرسالة) عن الغرباء.	المحتوى ذو القيمة الزمنية المحدودة عمومًا. يحتاج إلى ملف ناقل (وعاء) .
التشفير	جعل المحتوى الرقمي (الرسالة) غير مفهوم (واضح) للغرباء.	المحتوى ذو القيمة الزمنية المحدودة عمومًا. لا حاجة إلى ملف ناقل (وعاء) .
العلامات المائية	حماية المحتوى الرقمي للناقل (الوعاء)	قد يكون من السهل اكتشافه أو لا يكون. المتانة ضرورية .

11 – التورية: (Steganography)

11-1 أنواع التورية (الاخفاء)

يمكن تضمين محتوى الرسائل المخفية (النص الصريح) في الملف الناقل بثلاثة أنواع من الطرق. يمكن حقن الرسالة المخفية (النص الصريح) داخل الناقل، وهو ما لا يغير المحتوى الرقمي للناقل نفسه. أو يمكن استبدال جزء من محتوى الناقل الرقمي بالرسالة المخفية. وهذه الأخيرة تغير المحتوى الرقمي للناقل. وهناك طريقة جديدة نسبيًا لإخفاء المحتوى وهي استخدام الرسالة المخفية لإنشاء ملف جديد تمامًا ينقلها (الوعاء).

11-1-1 تقنيات الحقن

تورية (إخفاء) المعلومات في الملفات الموجودة يحدث بشكل روتيني في تطبيقات الحاسوب الشائعة. يتم تسجيل خصائص مستندات ميكروسوفت اوفيس (Microsoft Office) تلقائيًا بالمعلومات المحددة عندما تم تثبيت تطبيق (Office). يتم استخراج خصائص المؤلف تلقائيًا من معلومات المستخدم ضمن قائمة الأدوات/الخيارات، تتطلب الإزالة الكاملة الآمنة أدوات خاصة.
وبشكل أكثر عمدًا، يمكن إخفاء المعلومات بشكل غير مرئي في صفحات الويب باستخدام علامة "مخفي". لا يعرض العرض العادي لصفحة الويب المحتوى، لكن عرض المصدر يكشف عن علامة <input type="hidden"> . تشمل الأمثلة الأخرى تخزين البيانات في مساحة غير مستخدمة في مقدمة الملفات، وحزم البيانات المرسلة عبر الشبكات، ومساحة القرص غير المستخدمة. ومع ذلك، فإن استخدام المساحة المفتوحة دون أي تعديل على ملف الحامل محدود للغاية. لذلك، تتضمن التقنيات الأكثر حداثة وأمانًا بعض مستويات من التعديل للملف الناقل.

11 – التورية: (Steganography)

11-1-2 **تقنيات الاستبدال** : في تقنيات الاستبدال، يتم استبدال كمية محدودة من بيانات ملف الناقل بالمحتوى الرقمي (مشفر) للرسالة المخفية. في التقنيات التي تستخدم خوارزمية البت الأقل أهمية (LSB) ، يتم تغيير التمثيل الثنائي لكل عنصر صورة (بكسل) في ملف رسومي (مشفر) للرسالة المخفية. يتم ذلك بحيث يكون التأثير على الصورة المرئية ضئيلاً. ضع في اعتبارك ترميز الألوان التالي:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

يمكن لخوارزمية البت الأقل أهمية (LSB) إخفاء الثنائيات التسعة التالية **101101101** عن طريق تغيير الثنائي الأخير في كل ثمانية خانات (بايت) حسب الحاجة. يؤدي هذا إلى

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

يوضح هذا المثال أنه لإخفاء تسعة خانات ثنائية (بت) من المعلومات، تحتاج الخوارزمية فقط إلى تغيير أربعة من الثمانيات (بايت) التسعة الأقل أهمية في هذه الثمانيات التسعة. ولأن تغيير الخانة الأخيرة يسبب تغييرًا صغيرًا جداً جدً في لون البيكسل، فإن التغيير في الصورة غير محسوس للعين البشرية .

تتضمن تقنيات التورية في الملفات الصوتية باستخدام خوارزميات الأكثر تعقيدًا مثل : تحويل جيب التمام المنفصل (DCT)، وتحويلات فوريير، (إخفاء) المعلومات استبدال أطوار المقاطع القصيرة بشكل غير محسوس بأطوار مرجعية تمثل البيانات المخفية (ترميز الطور)، ونشر إشارة النطاق الضيق للرسالة على طيف واسع من الترددات مما يجعلها تبدو كضوضاء عشوائية (ترميز الطيف المنتشر)، وتقسيم عرض النطاق الترددي للناقل إلى قنوات متعددة والقفز بين هذه القنوات (القفز الترددي)، والعديد من التقنيات الأخرى.

11 – التورية: (Steganography)

11-1-3 **إنشاء الملف** : أخيرًا، يمكن استخدام رسالة المخفية لإنشاء ملف جديد تمامًا يبدو بريئًا. في الأساس، تنشئ الرسالة حاملها الخاص. ومن الأمثلة على هذه التقنية تطبيق (SpamMimic). باستخدام هذا التطبيق يمكن بسهولة إخفاء رسالة قصيرة في نص يبدو وكأنه بريد عشوائي. يمكن بعد ذلك إرسال هذه الرسالة إلى شخص ما يستخدم بعد ذلك موقع الويب لفك تشفير (فك الاخفاء) الرسالة. تتمثل ميزة هذا في أن قِلة من الناس قد يشككون في رسائل البريد العشوائي. هذه التقنية غير فعّالة نسبيًا، كما يتضح من تحويل الكلمات الثلاث "التخفي مثير للاهتمام" إلى نص يحتوي على عدد كلمات يبلغ (574) كلمة. تتضخم جمل الرسالة المراد اخفائها بسهولة إلى رسائل بريد إلكتروني تحتوي على آلاف الكلمات. ومع ذلك، نظرًا لمزايا هذه الطريقة، فقد لا يكون عدد الكلمات ذا أهمية كبيرة.

11-2 **مستويات تشفير الإخفاء**

يمكن أيضًا تمييز تقنيات الإخفاء من خلال مستوى التشفير. المستوى الأقل أمانًا، والذي لا يتطلب تبادل شفرة مثل مفتاح الإخفاء، هو **الإخفاء الكامل**. تعتمد فعالية الحفاظ على أمان رسالة الإخفاء فقط على قدرة الرسالة على البقاء دون اكتشاف. إن استخدام مفتاح الإخفاء السري قبل الاتصال يجعل الرسالة أكثر أمانًا، ولكنه قد يثير الشكوك أيضًا لأن تبادل مفتاح الإخفاء السري يجب أن يسبق نقل الناقل للرسالة المخفية. وبالتالي، هناك مقايضة بين احتمال الكشف من ناحية وأمان الرسالة المضمنة إذا تم اكتشافها. تستخدم التقنية الأكثر أمانًا مفتاحًا خاصًا ومفتاحًا عامًا لتأمين الرسالة المضمنة في الناقل. يتم تضمين رسالة المخفية باستخدام مفتاح عام، ويتم استخراج الرسالة المخفية باستخدام مفتاح خاص. كما هو الحال في تشفير بالمفتاح العام، ليست هناك حاجة لتبادل المفاتيح وبالتالي لا يزداد خطر الكشف. ويجب التأكيد أيضًا على أن المفاتيح في التخفي باستخدام المفتاح السري والتخفي باستخدام المفتاح العام لا تعمل إلا على تعزيز تنفيذ تطبيق التخفي باستخدام المفتاح العام، ولا تشكل استخدامًا للتشفير. يتضمن الجدول التالي ملخصًا لتقنيات التخفي.

11 – التورية: (Steganography)

الجدول : تقنيات التخفي

التقنية	الطريقة	التأثير على الملف الناقل	الملاحظات
تقنيات الحقن	استخدام أدوات تسجيل تضمن معلومات أو استغلال مساحة "شاغرة/مفتوحة" بالملف الناقل	عدم تغيير المحتوى	سعة إخفاء محدودة للغاية
تقنيات الاستبدال	تم تغيير جزء من المحتوى الرقمي للملف الناقل ليعكس رسالة المخفية	تدهور جودة محتوى الملف الناقل إلى حد ما	زيادة خطر الكشف مع زيادة حجم محتوى الرسالة المخفية
إنشاء ملف ناقل	رسالة التخفي مخفية في كمية أكبر من المحتوى رقمي جديد غير ذي الصلة (ملف ناقل جديد)	لا يوجد ملف ناقل جديد تم إنشاؤه	غير فعال، خطر الكشف يعتمد بشكل كبير على سياق الرسالة المخفية
تشفير التخفي	يتم تشفير محتوى الرسالة المخفية حيث أنه مدرج في الملف الناقل.	ليس التخفي الخالص	تبادل المفاتيح يزيد من خطر الكشف

11 – التورية: (Steganography)

11-3 أنواع الملفات

أخيرًا، يمكن للتخفي استخدام أنواع مختلفة من الملفات. وحتى وقت قريب، كانت الملفات السمعية البصرية تُستخدم في الغالب كملفات حاملة لتضمين محتوى الرسالة المخفية. وعادةً ما تكون هذه الملفات كبيرة الحجم وتتمتع بقدرة كبيرة على إخفاء المعلومات. على سبيل المثال، يمكن تغيير لون بكسل في أيقونة بشكل غير محسوس عن طريق تغيير رمز اللون الرقمي بشكل طفيف

(على سبيل المثال من 01011011 01010011 01011001 إلى 01011010 01010011 01011001)،

في حين أن تغيير حرف واحد في كلمة (fat) إلى (bat) ليس ملحوظًا فحسب، بل يغير أيضًا المعنى الكامل للكلمة. بالمناسبة، يتم تمثيل كليهما بثلاثة ثمانيات. ونظرًا لأن التخفي يُنظر إليه بشكل متزايد كأداة عمل مفيدة، يتم الآن استخدام أنواع أخرى من الملفات كملفات حاملة (غلاف).

11-4 تحليل الاخفاء

كما يمكن استخدام التقنيات الرقمية لإخفاء الرسائل، يمكن ايضا استخدامها للكشف عن الرسائل المخفية وفك شفرتها. تحليل الاخفاء هو عملية البحث عن الانحرافات الصغيرة في الأنماط المتوقعة لملف ما، بحيث يمكن الكشف عن وجود رسائل مخفية. تحليل الاخفاء والاخفاء (التورية) هما وجهان لعملة واحدة، على غرار التشفير وتحليل الشيفرة، والفيروسات الحاسوبية وبرمجيات مكافحة الفيروسات. تتضمن الابحاث في علم الاخفاء (التورية) تطوير تقنيات جديدة لإخفاء المحتوى وتطوير أدوات جديدة للكشف عن المحتوى المخفي وفك شفرته.

11 – التورية: (Steganography)

11-5 أنواع تحليل الاخفاء

استنادًا إلى معرفة الرسالة الفعلية (الرسالة المراد اخفائها)، وتوفر الملف الحامل الأصلي (الغلاف)، وأداة الاخفاء ، يمكن التمييز بين الأنواع التالية من التحليل الخفي:

- هجوم الاخفاء فقط - تتوفر الرسالة المخفية فقط للتحليل (النص المخفي)؛
- هجوم الغلاف المعروف - يتوفر كل من الغلاف (الملف الناقل) والنص المخفي؛
- هجوم الرسالة المعروفة - تكون الرسالة معروفة ويمكن مقارنتها بالنص المخفي؛
- هجوم الاخفاء المختار - يتوفر النص المخفي وأداة الاخفاء (الخوارزمية) للتحليل؛
- هجوم الرسالة المختارة - اختيار رسالة عادية، وتحويلها إلى رسالة تورية (إخفاء) لمزيد من التحليل؛
- هجوم الاخفاء المعروف - يتوفر النص الخفي وأداة الاخفاء (الخوارزمية) ورسالة الغلاف (الملف الحامل) للتحليل.

بشكل عام، يصبح التحليل الخفي أكثر كفاءة وفعالية كلما زادت العناصر المعروفة. يتم تقديم مستوى آخر من التعقيد مع انتقال التحليل الخفي من الكشف فقط إلى الكشف عن رسالة الخفاء وفك شفرتها.

11-6 الكشف عن الاخفاء

يمكن أن يعتمد الكشف عن الاخفاء (التورية) على مقارنات بين ملف الاخفاء والملف الأصلي، والكشف عن الملفات ذات أحجام أكبر من المتوقع، والاختلاف في الخصائص الإحصائية للمعلومات الرقمية في الملف. غالبًا ما لا تتوفر الملفات الأصلية، ما لم تكن واردة من مصادر عامة. ومع ذلك، تعمل العديد من تقنيات الاخفاء على زيادة حجم ملف الناقل الرقمي، إلى الحد الذي يصبح فيه ذا أهمية إحصائية. وعلاوة على ذلك، نظرًا لأن بنية الرسالة المخفية مركبة على بيانات الناقل الرقمية، فإن تحليل توزيع الخصائص المعروفة لبيانات الرقمية للناقل غالبًا ما تكشف عن وجود الرسالة المخفية. على سبيل المثال، يجب الاشتباه في ملفات الخريطة النقطية التي تحتوي على أكثر من 50 لونًا متطابقًا تقريبًا بأنها تحتوي على رسائل مخفية.

11 – التورية: (Steganography)

11-7 الاتلاف مقابل فك التشفير

أخيرًا، ليس فك تشفير رسائل التخفي ضروريًا دائمًا. إذا كان من الممكن تدمير الرسالة المخفية قبل وصولها إلى وجهتها، فإن محاولة الاتصال المخفية قد تم إحباطها فعليًا. يمكن تغيير الملفات الرسومية عن طريق تغيير تنسيقات الملفات وخوارزميات الضغط ومستويات الضغط، وعادةً بدون تأثير مرئي ملحوظ على سلامة ملف الناقل. باختصار، فإن اكتشاف وفك تشفير المحتوى المخفي معقد ويواجه العديد من التحديات. ومع ذلك، فهو موضوع لا يمكن للمجتمعات الأمنية والقانونية تجاهله.

علم التورية (Steganography) له عدد من العيوب عند مقارنته بالتشفير، حيث يتطلب الأمر الكثير من التكلفة لإخفاء أجزاء قليلة نسبيًا من المعلومات ، على الرغم من أن استخدام طريقة مثل المقترحة في الفقرة السابقة قد يجعله أكثر فعالية. أيضًا ، بمجرد اكتشاف النظام ، يصبح عديم القيمة تقريبًا. ويمكن التغلب على هذه المشكلة إذا كانت طريقة التضمين تعتمد على نوع من المفاتيح السرية، حيث يمكن تشفير الرسالة أولاً ثم إخفاؤها باستخدام إخفاء المعلومات.

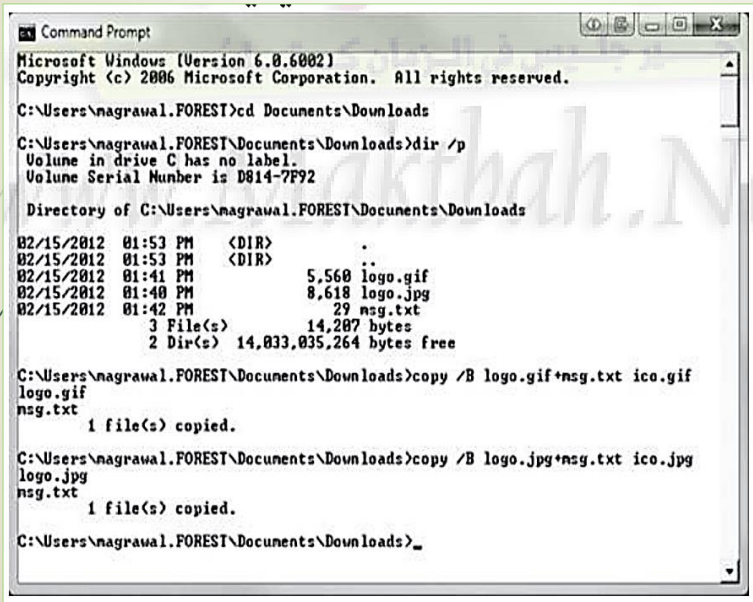
ميزة إخفاء المعلومات هي أنه يمكن استخدامها من قبل الأطراف التي لديها ما تخسره في حالة اكتشاف حقيقة اتصالاتهم السرية (وليس المحتوى بالضرورة)، حيث يشير التشفير إلى حركة المرور على أنها مهمة أو سرية أو قد تحدد المرسل أو المستلم كشخص لديه شيء يخفيه.

11 – التورية: (تمرين)

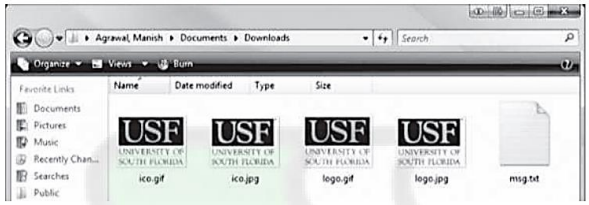
وهناك العديد من الطرق للقيام بالإخفاء لكن في هذا التمرين سنستخدم طريقة سهلة ومباشرة. سوف تقوم بإخفاء النص مع المعلومات ذات العلاقة داخل صورة (شعار الكلية على سبيل المثال) ومن ثم إرسالها إلى أصدقائك. وإذا كان أصدقاؤك يعلمون أين يبحثون فإن بإمكانهم بسهولة الحصول على المعلومات. والهدف من هذا التمرين هو توضيح مدى سهولة إنشاء تحديات لأمن المعلومات ومن ثم مدى صعوبة القضاء على مشاكل أمن المعلومات. وللقيام بهذا التمرين ستحتاج إلى ما يلي: ملف صورة: في حين أن أي ملف صورة سيؤدي الغرض، يفضل أن يكون ملف الصورة صغيراً من نوع (jpg) أو (gif). وعادة صورة شعار كليتك سيؤدي الغرض. احفظ الملف على حاسوبك. وفي هذا التمرين نفرض أن يتم حفظ جميع الملفات في مجلد التنزيلات لأنه موقع ملائم على كل الحواسيب. ولهذا المثال سيكون اسم ملف الصورة (logo.gif) إذا كان نوع الصورة "gif" أو (logo.jpg) إذا كان نوع الصورة "jpg". ملف ثاني يحتوي على تاريخ ومكان ووقت الاجتماع: احفظ الملف في المجلد نفسه الذي فيه ملف الصورة أعلاه وأسهل طريقة لإنشاء هذا الملف عن طريق برنامج المفكرة (Notepad) ومن ثم كتابة النص وحفظ الملف في مجلد التنزيلات. ولهذا المثال سيكون اسم الملف (msg.txt) .

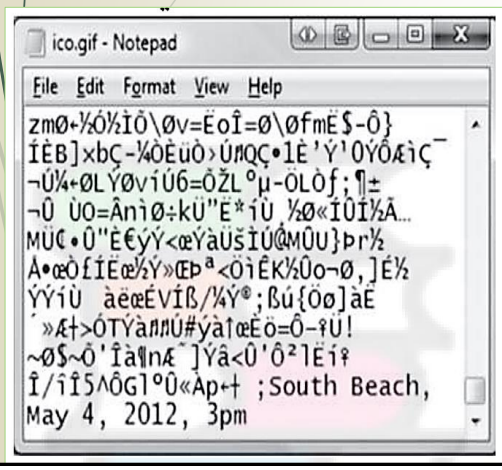
11 – التورية: (تمرين)

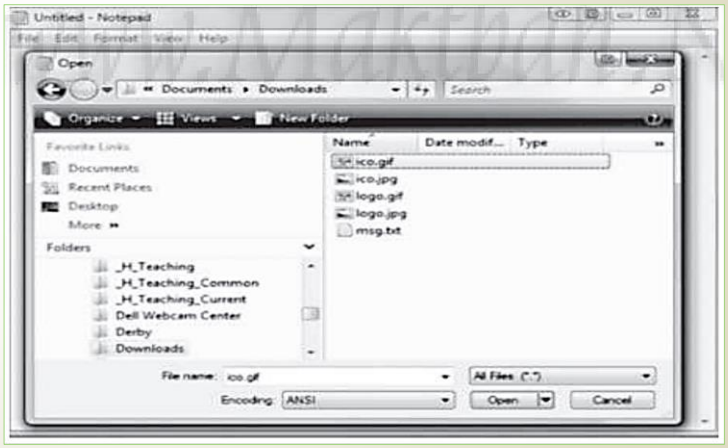
أوامر إخفاء ملف نصي في نهاية ملفات الصور



11 – التورية: (تمرين)







لينكد ان : أبريل 2021 ، التأثير: أكثر من 700 مليون سجل مستخدم مع حوالي 750 مليون مستخدم في عام 2021، تمكن المتسللون من نشر هويات المستخدمين لحوالي 700 مليون شخص (> 93٪ من إجمالي قاعدة المستخدمين) بعد إجراء عملية استخلاص للبيانات من موقع (LinkedIn) الإلكتروني. على الرغم من أن معظم المعلومات كانت متاحة للعامة، إلا أن إجراء عملية مسح للبيانات من خلال استغلال واجهة برمجة تطبيقات (LinkedIn) يعد انتهاكًا لشروط الخدمة. وشملت البيانات المحذوفة: الأسماء الكاملة، أرقام الهواتف، عناوين البريد الإلكتروني (الغير متاحة للعامة)، أسماء المستخدمين، سجلات تحديد الموقع الجغرافي، الجنس، تفاصيل حسابات وسائل التواصل الاجتماعي المرتبطة. ومن المحتمل أن تكون أي عناوين بريد إلكتروني يتم الكشف عنها أثناء الاختراق عرضة لبرامج الفدية أو هجمات التصيد الاحتيالي. على الرغم من أن البيانات كانت متاحة للجمهور، إلا أنها أثارت مخاوف بشأن أمن المعلومات وكيف يمكن لأطراف ثالثة استخدام تلك المعلومات لإنشاء قواعد بيانات (OSINT) (استخبار مفتوح المصدر). كما أنه يوفر فرصة للجهات الفاعلة السيئة لاستهداف الأفراد البارزين أو المديرين التنفيذيين للشركات. على سبيل المثال، حاول قراصنة صغار بسرعة استغلال هذه الحادثة، حيث ادعى أحد المستخدمين بأنه قام ببيع مجموعة جديدة من بيانات (LinkedIn) في منتدى عام مقابل ما قيمته 7000 دولار من عملة البيتكوين.

الفيسبوك : أبريل 2021 ، التأثير: انكشاف 530 مليون مستخدم ، على الرغم من أنها واحدة من أكبر الشركات في العالم، إلا أن فيسبوك ليس غريبًا على تسرب البيانات. لقد تعامل عملاق وسائل التواصل الاجتماعي باستمرار مع الخروقات الأمنية لبيانات المستخدم منذ طرح الشركة للاكتتاب العام في عام 2012. كان الاختراق الضخم للبيانات الذي تعرضت له الشركة في أبريل 2021 أحد أكبر تسريبات الأسماء وأرقام الهواتف وأسماء الحسابات وكلمات المرور لأكثر من 530 مليون شخص للجمهور. وحدد فيسبوك المشكلة في أداة النظام الأساسي لمزامنة جهات الاتصال، مشيرًا إلى استغلال المتسللين لثغرة أمنية لاستخراج ملفات تعريف المستخدمين للحصول على بيانات العملاء. على الرغم من تأكيد فيسبوك أنه لم يتم اختراق أي بيانات أو إساءة استخدامها، إلا أنه من المستحيل التحقق منها نظرًا لأن المعلومات كانت علنية لفترة قصيرة. يمكن للمتسللين أو المحتالين استغلال المستخدمين المطمئنين بسهولة من خلال أسمائهم وأرقام هواتفهم وعناوين بريدهم الإلكتروني فقط. منذ عام 2013، واجه فيسبوك العديد من خروقات البيانات الرئيسية، بما في ذلك: في مارس 2019، تسربت معلومات مفادها أن موظفي فيسبوك تمكنوا من الوصول إلى أكثر من 600 مليون حساب مستخدم. تم تخزين معرفات الحسابات وكلمات المرور لكل من (Facebook) و (Instagram) في ملفات نصية عادية. على الرغم من أن فيسبوك يزعم أنه لم يتم الكشف عن أي معلومات حساسة، إلا أن ذلك كان حادثًا آخر من بين العديد من المشكلات الأمنية. في أبريل 2019، اكتشف فريق (Cyber Risk) في (UpGuard) 540 مليون سجل بيانات مستخدم (Facebook) غير آمن على خوادم (Amazon S3) السحابية العامة. فشل مطور تطبيقات الطرف الثالث وشركة الإعلام المكسيكية (Cultura Colectiva) في حماية مجموعة البيانات بالكامل بكلمة مرور، مما ترك المعلومات مفتوحة لأي شخص للوصول إليها وتنزيلها. وعلى الرغم من أن فيسبوك لم يكن مسؤولاً بشكل مباشر عن هذا الحادث، إلا أنه سلط الضوء على كيفية إدارة الشبكة الاجتماعية لوصول طرف ثالث إلى قاعدة بياناتها. بعد تاريخ طويل من تسرب البيانات، قام فيسبوك أخيرًا بزيادة القيود المفروضة على مطوري الطرف الثالث. وبعد بضعة أشهر فقط، تم العثور على المزيد من السجلات المكشوفة على خادم أجنبي على شبكة الإنترنت المظلمة. توصل المزيد من التحقيقات إلى أن مجموعة من المتسللين في فيتنام ربما أساءت استخدام واجهة برمجة تطبيقات فيسبوك وسرقت الموقع بحثًا عن معرفات المستخدمين والأسماء وأرقام الهواتف. تأثر أكثر من 300 مليون مستخدم.

فيسبوك / كامبريدج أناليتيكا : أبريل 2018، التأثير: تعرض 50-90 مليون مستخدم في عام 2018، قامت شركة الاستشارات البريطانية، كامبريدج أناليتيكا، بسرقة وبيع بيانات من 50 إلى 90 مليون حساب مستخدم على فيسبوك في واحدة من أكثر الحالات شهرة في الذاكرة الحديثة. تمكن الباحث الأمني في (Cambridge Analytica Aleksandr Kogan) من الوصول إلى هذه البيانات من خلال ثغرة من تطبيق اختبار تابع لجهة خارجية. سمحت هذه الثغرة في واجهة برمجة التطبيقات (API) الخاصة بفيسبوك لـ Koganبتجميع البيانات من أي شخص قام بتنزيل التطبيق ومن شبكة أصدقائه بالكامل. على الرغم من مخالفة شروط وأحكام فيسبوك، واصلت *كامبريدج أناليتيكا* بيع البيانات بشكل غير قانوني لأنه لم يكن هناك تطبيق للقواعد. تشير التقارير إلى أن فيسبوك كان على علم بهذه المشكلة في وقت مبكر من عام 2015، لكنه لم يتخذ أي إجراء حتى أطلق كريستوفر ويلي، أحد موظفي *كامبريدج أناليتيكا*، صافرة الإنذار. وصلت الأمور أخيرًا إلى ذروتها عندما أعلنت لجنة التجارة الفيدرالية (FTC) عن غرامة تاريخية بقيمة 5 مليارات دولار بسبب انتهاك فيسبوك المستمر لأمن البيانات وممارسات حماية البيانات الضعيفة. كما فرضت لجنة التجارة الفيدرالية (FTC) عملية إعادة هيكلة كاملة من الأعلى إلى الأسفل لزيادة الإشراف على الامتثال للخصوصية. علاوة على ذلك، رفعت لجنة التجارة الفيدرالية دعوى قضائية ضد *كامبريدج أناليتيكا*، مما أجبر الرئيس التنفيذي **ألكسندر نيكس** على الاستقالة.