الفصل الأول

مفاهيم

يَشرَح هذا الفصل عددًا من المفاهيم الأساسيَّة في حقل أمن المعلومات، ويطرح مفاهيم أساسيَّة أخرى؛ لكي يكون القارئ مُمهَّدًا للتَعرُّف إلى الأفكار الواردة في هذا الكتاب.

1.1 أمن المعلومات

لقد تَعدَّدت التعاريف الرسميَّة لأمن المعلومات، وفيما يأتي تعريف أمن المعلومات المتوافِق مع اتِّجاهات هذا الكتاب. فأمن المعلومات Information security هو مُمارسَةُ العمل الذي يَتمثَّل في حماية المعلومات الخاصَّة من السرقة، أو الإفشاء، أو التخريب وإدخالها في وَضْعِ الأمان والمحافظة عليها، وتَقتَضي حماية المعلومات في هذا التعريف حماية محيطها ومحيط مالِكها أيضًا.

دورة حياة أمن المعلومات

2.1 أمان المعلومات

يحاول هذا الكتاب التمييز بين المصطلحَين (أمن المعلومات) و(أمان المعلومات)، حيث يَعدّهما بعضهم ذَوَي معنى واحد، ويَستنِد هذا الكتاب على مفهوم أن (أمان المعلومات) مختلِف عن (أمن المعلومات)، وإن (أمان المعلومات) Information safety، بالتعريف، هو الحالة (أو الوَضْع) التي تَدخُل فيها المعلومات الخاصَّة بعد اتخاذ إجراءات أمن المعلومات (أي بعد حمايتها من السرقة أو الإفشاء أو التخريب)، واتخاذ الإجراءات المستمرة لضمان أمان هذه المعلومات والتعامل مع المستجدات.

وكما تَمَّ تعريف (أمن المعلومات) فهو مُمارسَة عمل لحماية المعلومات الخاصَّة، أمّا (أمان المعلومات) فهو ضمان وَضْع المعلومات الخاصَّة بعد تأدية دور (أمن المعلومات). إنَّ مفهوم (أمان المعلومات) مهمٌّ للتمييز بين وَضْع المعلومات قبل تأدية وظيفة (أمن المعلومات) وبَعدها.

3.1 الطَرَف

الطّرَف هو الكائِن الذي يَتعامَل مع البيانات، سواء أكان فردًا Individual أم منظَّمةً Organization أم دولةً State أم طَرَفًا دوليًّا International party. والطّرَف الدولي هو مجموع دولتين أو أكثر.

4.1 الأصول الماديَّة والأصول غير المادية

الأصول الماديَّة Physical assets هي كُلُّ شيء مَلموس تَعود ملكيته إلى طرفٍ ما، مثل التجهيزات والشبكات وغيرها. أمّا **الأصول غير المادية** Logical assets فهي البيانات والمعلومات التي يَمتلِكها طرفٌ ما، ويَسعى العامِلون في حقل أمن المعلومات إلى حماية كلٍّ من الأصول الماديَّة والأصول غير المادية أيضًا.

5.1 البيانات والمعلومات

ثَمَّة اختلاف بين مصطلَحَي البيانات والمعلومات، فمن الناحية العامَّة في حقل تكنولوجيا المعلومات وَضَّحت بعض المراجع الفرق بين البيانات والمعلومات على أنَّ البيانات هي الحقائق (أو البيانات) الخام غير المنظَّمة وغير الجاهزة للاستعمال التي لم تُعالَج بعد، أمّا المعلومات فهي البيانات التي عولجت ورُتّبت، والتي أصبحت جاهزة للاستعمال [8، 7].

وفيما يلي تعريف لكلٍّ من البيانات والمعلومات يُوضِّح الفرق بينهما في سياق أمن المعلومات، **فالبيانات** Data هي مجموع المواد (الرقميَّة أو الورقيَّة) الموجودة التي تَعود ملكيتها إلى طرفٍ ما، والتي تَضم معلومات أو حقائق أو كليهما، وقد تَكون هذه الحقائق إمّا واضحة أو غير واضحة، وقد تُستعمَل أو لا تُستعمَل، وقد يُستفاد منها أو لا، وهي لا تَحمِل قيمة فعليَّة عند أي طرف. أمّا **المعلومات** Information فهي جزء البيانات الواضح

والمفهوم الذي يُمكِن استعماله والاستفادة منه، والذي يَحمِل قيمة فعليَّة عند طرفٍ ما، وقد تَكون المعلومات بالنسبة إلى طرفٍ ما مجرَّد بيانات، وقد تَكون البيانات بالنسبة إلى طرفٍ ما معلومات، وليس بالضرورة أن تَكون المعلومات نصوصًا مكتوبةً، فقد تكون عبارة عن صور فوتوغرافيَّة، أو تسجيلات صوتيَّة، أو تسجيلات فيديويَّة، أو مخططات ورسوم.

ثَمَّة نوعان من المعلومات هما: معلومات **عاديَّة** ومعلومات **خاصَّة**، فالمعلومات العاديَّة هي المعلومات العامَّة المشتَرَكة مع الآخرين التي لا تَنطوي على أي منفعة خاصَّة بطرف دون طرف آخر، والتي لا تَضم موادّ تُؤذي أطرافًا إذا أدرَكَتها أو توصلت إليها أطراف أخرى، ومن أمثلة المعلومات العاديَّة معلومات علميَّة، ومعلومات أدبيَّة، ومعلومات طبيَّة، وأخبار، وبرامج تلفازية، وأفلام سينمائيَّة، وأناشيد، ومواد الكتب أو الصحف أو الأقراص الحاسوبيَّة العامَّة. أمّا المعلومات الخاصَّة فهي المعلومات المرتبِطة بطرفٍ ما، التي يَعدّها هذا الطرف خاصَّة به، ولا يُريد أن يُشارِكه أحدٌ فيها، ولا يُريد أن يَطَّلع أحدٌ عليها إلا من أراد، ويَبتغي حمايتها من السرقة، أو الإفشاء، أو التخريب، ويَهتَم حقل أمن المعلومات بحماية المعلومات الخاصَّة فقط، ولا يَهدُف إلى حماية البيانات أو حتى المعلومات العاديَّة. ولذلك، لا تَرى منشورات حقل أمن المعلومات ضرورة في إضافة كلمة (خاصَّة) بعد كلمة (معلومات). وعليه، فإذا وَرَدت في هذا الكتاب كلمة (خاصَّة) بعد كلمة (معلومات) أم لم تَرِد، فيُقصَد ضمنيًّا أنَّ هذه المعلومات هي معلومات خاصَّة.

وقد تَكون المعلومات الخاصَّة مشتَرَكةً مع طرف أو أطراف عدَّة، وتُسمَّى عندها **معلومات خاصَّة مشتَرَكة**، أو تكون غير مشتَرَكة مع أي طرف، وتُسمَّى عندها **معلومات خاصَّة غير مشتَرَكة**، والمعلومات الخاصَّة المشتَرَكة هي المعلومات الخاصَّة التي يَتشارَك في استثمارها العاملون لدى طرف واحد أو أكثر، مثل معلومات قطاع الأعمال الخاصَّة، والطرف الوحيد الذي يُجيز قانونيًّا التشارُك في استثمار المعلومات الخاصَّة واستعمالها هو مالِك المعلومات (أو القيِّم إذا كان موكَّلًا بذلك من قِبَل مالِك المعلومات)

وإليه تَعود المنفعة الماليَّة من استثمارها، وصفة المعلومات الخاصَّة المشتَرَكة أنها مَسموح نَقلها وتداولها بين المُجَاز لهم فقط. أمّا المعلومات الخاصَّة غير المشتَرَكة فهي المعلومات الخاصَّة التي لا يَتشارَك مالِكها باستثمارها مع أحد أيًّا كان، مثل المعلومات الفردية الخاصَّة غير الحسَّاسة، وصفة المعلومات الخاصَّة غير المشتَرَكة أنها ممنوع نقلها ومن غير المَسموح أن يَستعمِلها إلا مالِكها.

للمعلومات الخاصَّة المشتَرَكة شكلان هما: **معلومات خاصَّة مشتَرَكة معدَّة للتخزين**، و**معلومات خاصَّة مشتَرَكة معدَّة للنقل**، واختصارًا IFTSPI. والمعلومات الخاصَّة المشتَرَكة المعدَّة للتخزين هي المعلومات الخاصَّة التي يَتشارَك في استثمارها أطراف عدَّة داخل أجهزة التخزين، سواء أكانت مخزَّنة في محيط إلكتروني أم في محيط يدوي. أمّا المعلومات الخاصَّة المشتَرَكة المعدَّة للنقل فهي المعلومات التي يَتشارَك في استثمارها أطراف عدَّة من خلال تَبادُلهم لها يدويًّا أو عبر شبكات رقميَّة.

6.1 نماذج المعلومات الخاصَّة

ثَمَّة ثلاثة نماذج للمعلومات الخاصَّة هي: **المعلومات ذات القيمة الماديَّة**، و**المعلومات ذات القيمة المعنويَّة**، و**المعلومات ذات القيمة المَجازيَّة**. المعلومات ذات القيمة **الماديَّة** هي المعلومات التي يُمكِن أن تَعود بنفعٍ مالي عندما تُستثمَر آنيًّا (أي في وقتها) مثل المعلومات الفرديَّة الخاصَّة التي تَضمّ أرقام الحسابات المصرفيَّة ورقم التعريف الشخصي ومعلومات الأعمال الخاصَّة، ومالِك المعلومات ذات القيمة الماديَّة قد يكون فردًا أو رئيس منظَّمة (تجاريَّة أو صناعيَّة) أو مسؤولًا حكوميًّا بالتفويض إذا كانت ملكيَّة المنظَّمة عامَّة. أمّا المعلومات ذات القيمة **المعنويَّة** فهي المعلومات التي لا تُقدَّر بثمن والتي قيمتها فوق ماديَّة، أي إنَّ أهميَّتها وحساسيَّتها تَفوقان أي قيمة ماليَّة مهما بَلَغ مقدار هذه القيمة، مثل المعلومات المصنَّفة سريَّة لدى القطاع العام أو الخاص، والمعلومات الدولية المصنَّفة سريَّة، ومالِك المعلومات ذات القيمة المعنويَّة هو

افتراضًا القيِّم المَعني بحماية هذه المعلومات، سواء في الدولة أو في الطرف الدولي، ولكنَّ المالِك الحقيقي للمعلومات ذات القيمة المعنويَّة هو السلطات العليا التي تَحكُم الدولة أو السلطات العليا المشارِكة بالمعلومات في الطرف الدولي، وأمّا المعلومات ذات القيمة **المَجازيَّة** فهي المعلومات التي تَحمِل أهميَّة بالنسبة إلى طرفٍ ما، ولكنَّها لا تَحمِل أي قيمة ماديَّة، وليست ذات قيمة معنويَّة، ولكنَّها في الوقت نفسه مهمَّة بالنسبة إلى ذلك الطرف، وتُعدّ من خصوصياته، مثل كلمات المرور الخاصَّة بصناديق البريد الإلكتروني، والمذكِّرات الشخصية. ومعنى كلمة (مَجازيَّة) هو أنَّ هذه المعلومات مَجازًا لها قيمة.

القيمة الماديَّة للمعلومات هي المكافِئ المالي الذي يُمكِن أن يُعيده استثمار تِلْك المعلومات في وقتها، وهذه القيمة تُساوي ذلك المكافِئ المالي آنيًّا. أمّا القيمة المعنويَّة فتُساوي منطقيًّا الـ (1) إنْ وُجِدَت أو الـ (0) إنْ لم تُوجَد، وكذلك القيمة المَجازيَّة.

7.1 المعلومات الرقميَّة والمعلومات الورقيَّة

المعلومات الرقميَّة Digital information هي المعلومات المخزَّنة في الأنظمة الحاسوبيَّة على شكل ملفات اثنانية، مثل الوثائق والصور والتسجيلات الصوتيَّة والفيديويَّة. أمّا **المعلومات الورقيَّة** فهي المعلومات المكتوبة أو المطبوعة على الورق، ومنها الوثائق والرسوم الورقيَّة، وتَنطبِق بعض الإجراءات المضادَّة على المعلومات الرقميَّة فقط، ويَنطبِق بعضها الآخر على المعلومات الرقميَّة والورقيَّة معًا.

8.1 ملكيَّة المعلومات

يجري تحديد الأصحاب الحقيقيين للمعلومات من خلال مفهوم **ملكيَّة المعلومات** Information ownership. في حقل أمن المعلومات، ثَمَّة ثلاثة أطراف تَتعامَل مع المعلومات هي: **المالِك**، **والقيِّم** Custodian، **والمستخدِم**. المالِك أو مالِك المعلومات هو الطرف الذي يَمتلِك المعلومات، ويَمتلِك قيمتها (سواء أكانت ماديَّة أم معنويَّة أم

مَجازيَّة)، ولديه كامل الحريَّة المطلقة في التصرُّف بهذه المعلومات، ويَتحمَّل أعباء سرقتها أو إفشاءها أو تخريبها إذا كان مسؤولًا بشكلٍ مباشر عن تخطيط الإجراءات المضادَّة وتطبيقها. أمّا القيِّم فهو عادةً الطرف الذي يَقَع على عاتقه مسؤولية الحفاظ على المعلومات وصيانتها من سرقتها أو إفشائها أو تخريبها، ولديه حقُّ الوصول إلى هذه المعلومات، وهو مسؤول مسؤوليَّة كاملة عن سرقة المعلومات أو إفشائها أو تخريبها إذا قام بتخطيط الإجراءات المضادَّة وتطبيقها، ومسؤول مسؤولية التخطيط فقط إذا قام بتخطيط الإجراءات المضادَّة، ولكنَّه لم يَقُم بتطبيقها، وكان تطبيقها سليمًا، ومسؤول مسؤوليَّة التطبيق فقط إذا قام بتطبيق الإجراءات المضادَّة، ولكنَّه لم يَقُم بتخطيطها، وكان تخطيطها سليمًا. أمّا المستخدِم فهو أي طرف يَستعمِل المعلومات لتحقيق أهداف مالِكها (كالموظَّف مثلًا أو مستخِدم خارج المنظَّمة) وأُعطي حَقَّ الوصول إلى هذه المعلومات من المالِك والقيِّم أو من أحدهما.

يُدعَى الطرف المقابِل لمالِك المعلومات – الذي لديه مصلحة أو منفعة من النفاذ إلى تِلْك المعلومات بشكل يُؤذي المصالح الماديَّة أو المعنويَّة أو المَجازيَّة لمالِك المعلومات – الخصم، ويَجب على مالِك المعلومات أن يَفترِض وجود الخصم حتَّى ولو لم يَكُن أصلًا؛ لأنَّ الأولويَّة الأساسيَّة في حقل أمن المعلومات هي حماية المعلومات في ظل وجود الخصم، ولأنَّ وجود فن أمن المعلومات غير ضروري إذا لم يَكُن هناك خصم (إضافة إلى التهديدات غير البشريَّة).

9.1 محيط المعلومات ومحيط مالِك المعلومات

محيط المعلومات Information environment هو الإطار الفيزيائي الذي يَضمّ المعلومات، ويَحفَظها، ويعالجها. ثَمَّة شكلان لطبيعة عمل محيط المعلومات هما **محيط إلكتروني** و**محيط غير إلكتروني (يدوي)**. المحيط الإلكتروني هو المكان والتجهيزات التي تَضم المعلومات الرقميَّة، وتَحفَظها فقط، مثل نظام حاسوبي أو أي أجهزة تخزين

رقميَّة أو أجهزة شبكة الاتصال الحاسوبية. أمَّا المحيط اليدوي فهو المكان الذي يَضم المعلومات الورقيَّة، ويَحفَظها فقط، مثل الخزنة الحديديَّة أو حافظات الملفات والوثائق الورقيَّة وجميع وسائط حفظ المعلومات بشكلها غير الرقمي؛ أي ما يسمى analog. أمَّا **محيط مالِك المعلومات** Owner environment فهو الإطار الفيزيائي الذي يُحيط بمالِك المعلومات وبمحيط المعلومات معًا، مثل: حجرة أو منزل أو منظَّمة أو دولة، ويَقَع محيط المعلومات داخل محيط مالِك المعلومات، وهو جزءٌ منه.

10.1 مفهوم التعمية (التشفير) أهم تقنيات أمن المعلومات

من المفاهيم الأساسية التي تُشكِّل عماد أمن المعلومات والاتصالات التعمية أو التشفير، وعلى الرغم من وجود كثير من المفاهيم التعموية، إلا أننا سنُعرِّف في هذه الفقرة الأساسيات منها فقط، وسوف نَتحدَّث عن المصطلحات الأخرى لاحقًا.

التعمية Cryptography بالتعريف: **علم حماية المعلومات السرِّية**، وهذا التعريف يرتبِط بالهدف الرئيس للتعمية، وهو الحفاظ على سرِّية المعلومات. أمّا في التعريف الاصطلاحي **فالتعمية هي تحويل المعلومات السرِّية من الشكل الواضح المقروء والمفهوم إلى شكل آخر طُلسمي وعشوائي وغير مفهوم، وذلك باستخدام خطة محدَّدة تَكفُل استرجاعها وإعادتها إلى هيئتها الأصلية الواضحة.** يُدعَى الشخص الذي يُمارِس علم التعمية **المُعمِّي** Cryptographer، والمُعمُّون هم عادةً إمّا باحثين أو رياضيين أو مبرمجين، ويُطلَق لقب المُعمِّي على كل من يعمل، ويُسهِم في حقل التعمية، والاختصاصي في التعمية هو الشخص الذي يُصمّم الخطط التعموية، ويحدّثها، ويضع الآليات المرتبطة بها (البروتوكولات).

جاء مصطلح "Cryptography" أساسًا من الكلمتين اليونانيتَي الأصل: "Kryptos" التي تَعني (مَخفيَّة أو كامنة أو محجوبة)، و"graphy" التي تَعني الكتابة، وبضَمِّهما معًا تُصبِحان كلمة واحدة "Kryptos graphy" أي (الكتابة المَخفيَّة) أو كما في الاصطلاح

العربي التراثي (التعمية)، ولقد دَرَج في هذه الأيام استعمال كلمة (تشفير) بدلًا من كلمة (تعمية)، وقد أَطلَق العلماء العرب الذين عملوا بهذا المجال في القرون الوسطى مصطلحات أخرى تُرادِف (التعمية)، مثل (تعمية الحروف) و(الترجمة) و(الكتابة الباطنة)[1]، لكن تَظَل كلمة (التعمية) المقابِل العربي السليم لمصطلح "Cryptography".

يَتمثَّل دور التعمية في حماية المعلومات السرِّية Secret Information ذات الطبيعة الخاصة، وهي المعلومات التي لا نُريد أن يَطَّلع عليها الآخرون (إلا مَن أَرَدنا مشاركته فيها)، ولا يَهمُّنا تعمية المعلومات التي لا نَراها خصوصية، ولا يَستفيد منها خصم. في الواقع، ثمة نوعان من المعلومات السرِّية:

- معلومات سرِّية فردية (غير مُشترَكة) Non-shared Secret Information: وهي المعلومات السرِّية الخصوصية المرتبِطة بطرف واحد فقط، وهو الشخص المُرخَّص له بقراءتها واستعمالها، ومن أمثلة هذا النوع: أرقام الحسابات المصرفية، وكلمات السر الخاصة بالبريد الإلكتروني الشخصي، والمذكرات اليومية...
- معلومات سرِّية جماعية (مُشترَكة) Shared Secret Information: وهي المعلومات السرِّية المتعلِّقة بأكثر من طرف واحد، ومن صفاتها أنها مفهومة ومُشترَكة بين شخصين أو أكثر، ولكنها مع ذلك تُعدّ سرِّية على بقية الأطراف غير المَعنية وغير المَرخَّص لهم بقراءتها واستعمالها، ومن أمثلة هذا النوع: المراسلات التي تَتم على مستوى الحكومات، كالمراسلات الدبلوماسية، أو العسكرية، أو الأمنية، أو الاستخباراتية، والمراسلات التي تَتم على مستوى المنظمات والشركات، كالصفقات السرِّية التجارية المتبادَلة، إضافة إلى تلك التي تَتم على مستوى الأفراد، كالرسائل العائلية الخاصة، وغير ذلك.

---

(1) (التعمية واستخراج المعمى عند العرب)، مراياتي ومير علم والطيان، الجزء الأول، منشورات مجمع اللغة العربية بدمشق.

وبالنسبة إلى الوجهة (المكان المقصود) التي ستَستَقر فيها المعلومات السرِّية بعد تعميتها، فثمة خياران: إمّا تخزينها Storing (أو إبقاءها) على القرص لحين استرجاعها واستعمالها لاحقًا، مثل المعلومات السرِّية الفردية، أو إعدادها للإرسال عبر الشبكة، مثل المعلومات السرِّية الجماعية التي غالبًا ما تكون مُضمَّنة في رسائل البريد الإلكتروني.

تُسمَّى المعلومات السرِّية التي نُريد حمايتها (تعميتها) **النص الواضح** Plaintext، وتُسمَّى أيضًا **النص الصافي** Cleartext، وتقنيًّا يُشير مصطلح النص الواضح إلى أيّ بيانات نصية مكتوبة بمحارف[1] ASCII القياسية مثلًا، وهي قابلة للقراءة والفهم، وتَضم حروف الأبجدية الإنجليزية (الصغيرة والكبيرة) والأرقام والإشارات والرموز وبعض محارف التحكُّم، مثل المحرف tab، ومحرف بداية السطر الجديد، وذلك في أغلب برامج تحرير النصوص العادية وتطبيقاتها، مثل برنامج Notepad في نظام Windows[2]. أمّا في علم التعمية، فتُطلِق مصطلح (النص الواضح) على كل ما نُريد حمايته، فقد يكون النص الواضح في التعبير التعموي عبارة عن رسالة جهّزها طرفٌ ما، تحوي معلومات نصية فقط مقروءة ومفهومة وذات دلالة، ومكتوبة بحروف اللغة الطبيعية (الأبجدية)، وهي مُعدَّة وجاهزة للإرسال عبر الشبكة ليتلقَّاها طرف ثانٍ، وكما ذكرنا سابقًا، تَندرِج الرسالة التي تحوي معلومات سرِّية تحت سقف المعلومات السرِّية الجماعية، وغالبًا ما يكون محتواها أمورًا تَتعلَّق بإرشادات دبلوماسية أو صفقات تجارية أو علاقات عائلية أو أي شيء خاص ومُشترَك بين طرفين أو أكثر، وقد يكون النص الواضح (الذي نَرغَب في تعميته) أيضًا عبارة عن ملف File؛ ملف نصي txt مثلًا، أو ملف صورة bmp، أو

---

(1) يَختلِف مصطلح محرف character عن مصطلح حرف letter. فالمحرف يمكن أن يُمثِّل حرفًا letter أو رقمًا numeral أو رمزًا symbol أو محرف تَحكُّم control character، أمّا الحرف فهو جزء من أبجدية منتهية ومحدودة، مثل الأبجدية الإنجليزية. ويمكننا أن نُسمِّي الحرف محرفًا، لكن لا نستطيع تسمية المحرف حرفًا؛ لأن مجموعة المحارف أوسع، وهي تشمل مجموعة الحروف.

(2) من الآن فصاعدًا سيَقتصِر استخدامنا لمصطلح النص الواضح plaintext ليعني كل ما نُريد حمايته من البيانات، سواء أكانت مقروءة أم غير مقروءة.

ملف صوتي mp3، أو ملف فيديوي avi، أو ملف تنفيذي exe، أو حتى سلسلة من الخانات الاثنانية (البتَّات bits)، وبتعبيرٍ آخر ملف اثنانيّ binary file. وسواء أكانت المعلومات أو محتويات الملف المُراد حمايته وتعميته مقروءة (حروف أبجدية مفهومة) أم غير مقروءة (محارف عشوائية مثلًا) يُطلَق عليها وعلى الملف بأكمله مصطلح النص الواضح، وفي رياضيات التعمية يُعرَّف النص الواضح بأنه دَخْل تابع التعمية وخَرْج تابع فك التعمية، وفيما يَتعلَّق بوجهة الملف المُعمَّى، يَبقى الخيار متاحًا بين تخزينه على وسائط التخزين الرقمية المختلفة أو إرساله عبر الشبكة إلى طرف آخر.

إذًا، يُطلَق مصطلح النص الواضح plaintext في التعبير التعموي على كل ما نُريد حمايته من المعلومات السرِّية الموجودة في الحاسوب، سواء أكانت نص رسالة أم ملفًّا اثنانيًّا[1]. وعلى كُلٍّ، يُعبَّر عن النص الواضح في التعمية التطبيقية بالبتَّات فقط سواء أكان رسالة نصية أم ملفًّا اثنانيًّا.

أمّا المعلومات السرِّية التي تمَّ تحويلها (تعميتها) إلى الشكل الطِّلسمي العشوائي غير المفهوم فتُدعَى **النص المُعمَّى** Ciphertext، ونقصد بعبارتنا إلى شكل غير مفهوم أنَّ المعلومات لا يمكن قراءتها، وليس لها دلالة أو معنى إن كانت نص رسالة، ولا يمكن مشاهدتها إن كانت ملف صورة، ولا يمكن سماعها إن كانت ملفًّا صوتيًّا، ولا يمكن تنفيذها إن كانت ملفًّا تنفيذيًّا، أو بتعبيرٍ آخر، لا يمكن استعمالها بالشكل الذي هي عليه، ولن يَتمّ تمييز نوعية النص المُعمَّى ومضمونه بعد التعمية، سواء أكان رسالة نصية أم ملفًّا اثنانيًّا؛ لأنه في الحالتين عبارة عن محارف ورموز مركَّبة عشوائيًّا، وعلينا أن نُميِّز بين ملف مُعمَّى Encrypted file وملف اثناني Binary file، فقد لا يكون للملف الاثناني امتداد، عندها يَتبادَر إلى الذهن أنه ملف مُعمَّى، وأنَّ محتوياته هي نص مُعمَّى بمجرَّد رؤية البيانات العشوائية الداخلية، وهذا غير صحيح؛ لأنَّه ليس كل ملف يحوي بيانات

(1) اصطلح مجمع اللغة العربية بدمشق على هذا المصطلح (اثاني) لكلمة Binary لتمييزها عن (ثنائي).

عشوائية غير مفهومة هو ملفًّا مُعمَّى، فقد يكون هذا الملف إمّا ملفًّا مضغوطًا أو حتى ملفًّا اثنانيًّا، إلا إذا تمَّ التأكد من أنَّ محتوياته هي نص مُعمَّى فعلًا، وأنها ناتج تعموي عن خوارزمية ما، ونَستطيع أن نَعدّ النص المُعمَّى بمنزلة بيانات؛ لأنه يحتوي ضمنيًّا على معلومات نَستفيد منها بمجرَّد فك تعميته، وأيضًا يُعرَّف النص المُعمَّى رياضيًّا بأنه دَخْل تابع فك التعمية وخَرْج تابع التعمية.

يمكن استخدام المصطلح Cryptogram، الذي يَعني **رسالة مُعمَّاة**، بوصفه مُرادِفًا لمصطلح Ciphertext فقط في حال كان مضمون الناتج التعموي مجرَّد رسالة نصية عادية[1]؛ أي لا نستطيع أن نُطلِقه على ملف مُعمَّى، وبمجمل الأحوال، نُطلِق مصطلح النص المُعمَّى Ciphertext على كل ما هو ناتج تعمية، سواء أكان في الأصل رسالة نصية أم ملفًّا اثنانيًّا؛ لأنَّ كلًّا من النص الواضح والنص المُعمَّى في النهاية عبارة عن بتّات في التعمية التطبيقية.

تُدعَى الخطة أو الطريقة التي تَقوم بتحويل النص الواضح إلى نص مُعمَّى ثم تحويله (استرجاعه أو إعادته) إلى النص الواضح مرةً أخرى **المُعمِّي**[2] Cipher (وتُكتَب أيضًا Cypher)، والمُعمِّي هو في الحقيقة مجموعة محدَّدة من الخطوات (أو خوارزمية، ولذا يُعرَّف في معظم الأحيان **بخوارزمية التعمية** Cryptographic Algorithm، ويُعرَّف في أحيان أخرى **بخطة التعمية** Cryptographic Scheme) تَعمَل وفق آلية معيَّنة ومنهج دقيق، ويَستعمِل المُعمِّي المفتاح والنص الواضح عند عملية التعمية لإنتاج النص المُعمَّى، ويَستعمِل المفتاح والنص المُعمَّى عند عملية فك التعمية لاستخراج النص الواضح، ويجب أن يَضمَن المُعمِّي استعادة المعلومات الأصلية كما كانت (قبل تعميتها)

---

(1) حتى لو كانت الرسالة موجودة في ملف نصي txt لا يمكن تسمية الملف المُعمَّى الناتج بـ cryptogram.

(2) يجب التمييز بين كلمة (مُعمِّي) المقابلة لمصطلح cipher و(مُعمِّي) المقابلة لمصطلح cryptographer.

دون تغيير، ولو على مستوى حرف واحد (أو بت واحد). ورياضيًّا، يُعرَّف المُعمِّي بأنه الخوارزمية الرياضية mathematical algorithm المُستخدَمة للتعمية وفك التعمية.

جاءَت كلمة (Cipher) من كلمة عربية الأصل هي (الصفر)، وكانت تُستخدَم عادةً في اللغات الأوروبية، في القرون الوسطى بعد انتقال مفهوم الصفر العربي إلى هناك، للإشارة إلى شيء غامِض وغير مفهوم؛ لأن مفهوم الصفر كان غامضًا لهم بالمقارنة مع الترقيم الروماني السائد في تلك الحقبة، ففي القرون الوسطى بأوروبا، عندما أراد الناس التعبير عن أمرٍ مُبهَم كاللغز، كانوا يدعونه Cipher.

من أهم مكوِّنات النظام التعموي الأساسية **المفتاح** Key[1] (وهو اختصارًا لعبارة **المفتاح التعموي** Cryptographic Key). والمفتاح هو وحدة البيانات التي تَتحكَّم في ناتج التعمية في كل مرة يتم تغييره (وهذا أمر ضروري)، وعلى الرغم من أن المفتاح وحدة من البيانات، يُصنَّف في باب المعلومات (كالنص الواضح) وليس في باب البيانات مع أنَّ حروفه عشوائية في بعض الأحيان، والسبب في ذلك التصنيف أنَّ المفتاح هو الوسيلة الوحيدة لاسترجاع المعلومات بعد تعميتها، وهو يُعَدّ من المعلومات السرِّية التي يجب حمايتها، وكما ذُكِر سابقًا، فالمفتاح هو الجزء المُستخدَم مع النص الواضح لإنتاج النص المُعمَّى، والمُستخدَم مع النص المُعمَّى لاستعادة النص الواضح، وذلك في طَوْر عمليتين عكسيتين: الأولى تُدعَى التعمية، والثانية تُدعَى فك التعمية.

يمكن أن يكون المفتاح كلمة، وتُسمَّى عندها كلمة المرور أو كلمة السر Password، أو عبارة، وتُسمَّى عبارة المرور Passphrase، أو مجموعة من الأرقام، وبالنسبة إلى صيغة المفتاح (أو بيانات المفتاح) فقد تكون مَقروءة ومفهومة وواضحة، مثل الكلمات العادية البسيطة التي يَختارها المستخدِم ليَسهُل عليه حفظها، وتَتألَّف تلك الكلمات عادةً من

(1) في الحقيقة، فضاء المفتاح هو أحد مكوِّنات نظام التعمية، وليس المفتاح الواحد، إذْ إنَّ المفتاح الواحد هو جزء من ذلك الفضاء.

حروف أبجدية عادية، وأحيانًا مزيج من الحروف والأرقام، وفي بعض الأوقات تُصبِح طويلة لغرض زيادة السرِّية، وقد تكون صيغة المفتاح غير مفهومة وغير واضحة، مثل السلاسل المحرفية المركَّبة بشكل عشوائي من الحروف والأرقام والرموز، ولكنها مع ذلك قابلة للطباعة، ولكل خطة تعمية **طول مفتاح** Key Length ثابت يُدعَى أحيانًا **حجم المفتاح** أو طوله Key Size. في الواقع، لا تَعدّ خطة التعمية كلمةَ المرورِ أو عبارةَ المرورِ على أنها مفتاح التعمية وفك التعمية النهائي.

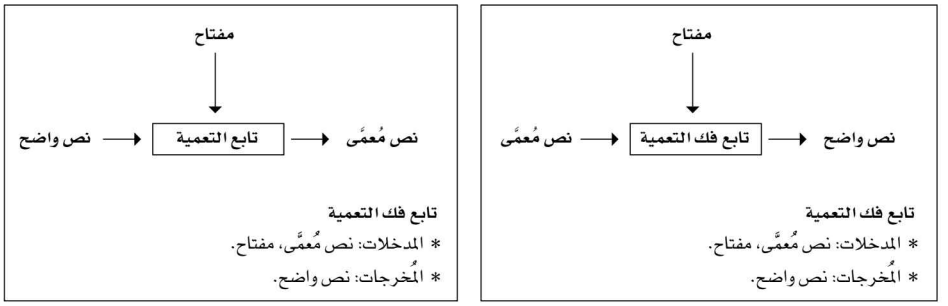
وبتعبيرٍ آخر، لا تَستعمِل خوارزمية التعمية السلاسل المحرفية المتغيِّرة الطول التي يُدخِلها المستخدِم مباشرةً، إنَّما تَقوم بإجراء عدد من العمليات عليها (كتوسيعها مثلًا) من أجل توليد بتّات المفتاح النهائي المستعمَلة لتنفيذ عملية التعمية وفك التعمية، وطول تلك البتات هو طول المفتاح الثابت، ويُسمَّى مجموع تلك العمليات عملية توليد المفتاح، ويَتم تنفيذها قبل تنفيذ عملية التعمية وفك التعمية، ورياضيًّا يُعرَّف المفتاح بأنه دَخْل تابع التعمية وتابع فك التعمية.

عملية التعمية Encryption هي عملية تحويل النص الواضح إلى نص مُعمَّى، وهي الجزء الأول من خطة التعمية. أمّا **عملية فك التعمية** Decryption فهي العملية العكسية التي تَقوم بتحويل النص المُعمَّى إلى نص واضح، وهي الجزء الثاني والمُكمِّل لخطة التعمية. وعلى نحوٍ أدق، عملية التعمية هي التابع الرياضي المستخدَم لتعمية النص الواضح، ويُسمَّى **تابع التعمية** Encryption function، ومُدخَلات تابع التعمية هي النص الواضح والمفتاح، ومُخرجاته هي النص المُعمَّى فقط.

أمّا عملية فك التعمية فهي التابع الرياضي المستخدَم لفك تعمية النص المُعمَّى، ويُسمَّى **تابع فك التعمية** Decryption function، ومُدخَلاته هي النص المُعمَّى والمفتاح ومُخرَجاته هي النص الواضح فقط. يُبيِّن الشكل (1-1) عمليتَي التعمية وفك التعمية من المنظور الرياضي، ويَرتبِط تابع فك التعمية بتابع التعمية وفق طريقة رياضية، بحيث

يُنفِّذ بدقَّةٍ تامة عكس ما يقوم به تابع التعمية، وذلك ليَضمَن استعادة المعلومات الأصلية الواضحة كما كانت، ويُرادِف مصطَلحَي encryption وdecryption مصطلحان آخران هما Encipherment وDecipherment على التوالي.

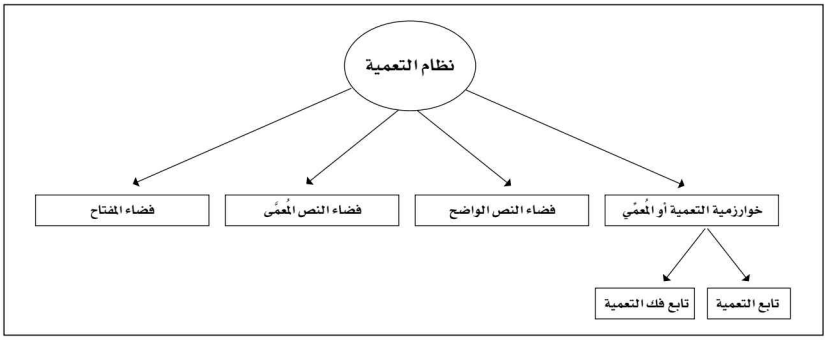
الشكل 1_1 عمليتَا التعمية وفك التعمية



يُشير المصطلحان **يُعمِّي**، و**يَفُك التعمية** إلى القيام بعمليتَي التعمية وفك التعمية، وثمة مصطلحان شائعان مرادفان يُؤدِّيان المعنى نفسه، هما Encipher وDecipher. تَستخدِم كتب التعمية ومراجعها زَوجَي المصطلحات السابقة بحسب الكاتب، والكتاب الذي يَستعمِل مصطلح (encrypt) ليَعني القيام بعملية التعمية يَستعمِل مصطلح (decrypt) ليَعني القيام بعملية فك التعمية، وكذلك هو الأمر بالنسبة إلى المصطلحين (encipher) و(decipher).

يَتكوَّن **نظام التعمية** Cryptosystem عمومًا من خوارزمية التعمية وإجمالي النصوص الواضحة والنصوص المُعمَّاة والمفاتيح الممكنة، ويُدعَى إجمالي النصوص الواضحة **فضاء النص الواضح** Plaintext Space، ويُدعَى إجمالي النصوص المُعمَّاة **فضاء النص المُعمَّى** Ciphertext Space، أمّا إجمالي المفاتيح الممكنة في المُعمِّي، فيُدعَى **فضاء المفتاح** Key Space، ويُقدِّم الشكل (1–2) صورة عن مُكوِّنات نظام التعمية.

الشكل (2_1) مخطط نظام التعمية.



بعد أن تَعرَّفنا إلى علم التعمية سنَتعرَّف الآن إلى علم (استخراج المعمى) كما سماه العرب واضعو هذا العلم[1] أو (تحليل التعمية) كما يسميه بعضهم الآن، **واستخراج المعمى** Cryptanalysis بالتعريف هو: **فَن وعلم اختراق حماية المعلومات السرِّية**، وبالتعريف العلمي **تحليل التعمية هو فك تعمية المعلومات السرِّية وتحويلها من الشكل العشوائي غير المفهوم إلى الشكل الواضح المقروء والمفهوم دون أي استخدام للمفتاح**، ويُمارِس هذا العلم مستخرج **التعمية** Cryptanalyst أو **مُحلِّلها**، وهو عادةً خبير في اللغة التي كُتِب بها النص الواضح، وفي الرياضيات التي تُعدّ الخبرة بها حاليًّا أكثر أهمية من اللغة بسبب تطبيق طرق التعمية المعقدة رياضيًّا.

إذًا، استخراج المعمى أو تحليل التعمية هو محاولة مُتعمَّدة لاستخراج النص الواضح من النص المُعمَّى دون امتلاك أو حتى معرفة بسيطة بالمفتاح الذي استُعمِل في تعميته، وتَتضمَّن المحاولة استخدام تقنيات عدة من أجل الوصول إلى الهدف المنشود، ويُشار إلى تلك المحاولة الموجَّهة في تحليل التعمية **بالهجوم** Attack، وثمة كثير من الأساليب والطرق لاسترجاع النصوص الواضحة، منها مثلًا كَشْف المفتاح المستخدَم،

---

(1) انظر: (علم التعمية واستخراج المعمى عند العرب) الجزءان الأول والثاني، منشورات مجمع اللغة العربية بدمشق، وترجمتهما للإنجليزية، منشورات مركز الملك فيصل للدراسات والبحوث الإسلامية.

أو إيجاد الحل العام، وقد يَتمّ الهجوم إمّا على نص مُعمَّى واحد فقط لاستعادة النص الواضح المقابل له أو على خطة التعمية المستخدَمة ككل؛ وذلك لاستعادة أي نص واضح، والمهمة الأصعب في الهجوم على خطة التعمية هي استنباط نقاط الضعف الموجودة بها واستغلالها في إيجاد طريقة عامة (الحل العام) لمعرفة المفتاح واستعادة النصوص الواضحة (أو استعادة النصوص الواضحة فقط دون الاهتمام بمعرفة المفتاح) بسهولة متى تَوافرت نصوص مُعمَّاة. أمّا حالة فقدان المفتاح من خلال حادثة لا تَتعلَّق أبدًا بتحليل التعمية (كإهماله أو إضاعته مثلًا) فتُدعَى **الافتضاح** Compromise.

بَقي علينا أن نُشير إلى وجود الفرق بين فك تعمية النص المُعمَّى وتحليل تعميته، فمن خلال فك تعمية النص المُعمَّى نَستعيد النص الواضح بواسطة استخدام المفتاح. أمّا من خلال استخراج تعميته فنَستعيد النص الواضح دون أي استعمال للمفتاح.

يُعرَف مصطلح تحليل التعمية أيضًا **باختراق المُعمِّي** Breaking a cipher، ويُطلِق الكثيرون في هذه الأيام مصطلحًا عاميًّا شائعًا يُفيد معنى تحليل التعمية هو (كسر الشيفرة). أمّا علماؤنا العرب الذين اشتغلوا بهذا المجال فقد أَطلَقوا تسميات عدة تُرادِف مصطلح تحليل التعمية، مثل (استخراج المُعمَّى) و(فك المُعمَّى) و(حل الترجمة) و(حل التعمية).

علم التعمية واستخراجها Cryptology **هو العلم الذي يَضُم كلًّا من علم التعمية وعلم تحليل التعمية.** جَوهَر هذا العلم هو الدراسة المشتركة للتعمية وتحليلها، ويُدعَى الشخص العامل في هذا المجال **خبير التعمية واستخراجها** Cryptologist. إنَّ عمل خبراء التعمية وتحليلها مُعقَّد جدًّا، حيث يقومون بتصميم خوارزميات وخطط التعمية، وفي الوقت نفسه يقومون بهجمات تحليلية عليها لاختبار قوتها والتأكد من حسن أدائها وسير عملها، وبكل تأكيد يَتطلَّب ذلك منهم الخبرة الرياضية الكافية، وسوف تَجِد

بعضهم يَستعمِل مصطلح (cryptology) بوصفه مرادفًا لمصطلح (cryptography) في بعض الحالات، وهذا خاطئ.

إنَّ استخدام التعمية لحماية المعلومات السرِّية الفردية ضَيِّق ومحدود جدًّا، وهو يقتصِر فقط على تأمين الملفات المخزَّنة على القرص؛ لئلا يقوم شخص آخر باستعمال الحاسوب والاطلاع على تلك الملفات؛ لذا فإنَّ أهم ما تُقدِّمه التعمية (وتقنياتها بلا شك) هو حماية المعلومات السرِّية الجماعية المتمثِّلة في الرسائل المتبادلة بين الأطراف المعنية.

يُعرَّف **الطرف** Entity أو **المُشارِك** Party بأنه جزء الاتصال القائم بين أطراف عدة، ومَهمّة الطرف قد تكون إرسال المعلومات أو استقبالها أو السيطرة عليها، وقد يُمثِّل هذا الطرف شخصًا ما أو محطة طرفية حاسوبية (مخدِّم)، وعندما تكون ثمة رغبة لدى طرفٍ ما في إنشاء رسالة سرِّية وتجهيزها للإرسال عبر الشبكة (مثل الإنترنت) إلى طرفٍ آخر، تَتشكَّل **بيئة الاتصال** Communication Environment أو **محيط الاتصال**، وتَتألَّف بيئة الاتصال بشكل افتراضي من ثلاثة مُشارِكين وقناة تبادل (إرسال واستقبال)، والمُشارِك الأول من بيئة الاتصال هو **المُرسِل** Sender، ويُعرَّف بأنه الطرف الأول من الاتصال القائم بين طرفين، وهو المُرسِل الشرعي الحقيقي للرسالة. أمّا المُشارِك الثاني من بيئة الاتصال فهو **المُستقبِل** Receiver، ويُعرَّف بأنه الطرف الثاني من الاتصال القائم بين طرفين، وهو المُستقبِل الشرعي المَعني بالرسالة، والمُشارِك الثالث من بيئة الاتصال هو **الخصم** Adversary، ويُعرَّف بأنه الطرف الثالث من الاتصال القائم بين طرفين، وهو الطرف غير الشرعي بينهم (الشاذ).

من الواضح أنَّ الخصم ليس المُرسِل أو المُستقبِل، إنّما هو دخيل لا علاقة له بالأصل في هذا الاتصال على خلاف المُرسِل والمُستقبِل، ويَقوم الخصم عادةً باختراق سرِّية (حماية) المعلومات المتبادَلة بين الطرفين الشرعيَين (المُرسِل والمُستقبِل)، وذلك من خلال أداء دور إمّا المُرسِل الشرعي أو المُستقبِل الشرعي أو كليهما، والهدف من قيامه بذلك هو قراءة الرسائل السرِّية المتبادَلة التي تَهمُّه، إضافة إلى التلاعب بهذه الرسائل

عن طريق تعديلها إمّا بإضافة معلومات مُزيَّفة أو بحذف معلومات محدَّدة أو تغيير بعض المعلومات، ويَتم كل هذا دون شك بعد أن يَتمكَّن الخصم من كَشْف مضمون الرسالة وقراءتها، ويُطلَق على الخصم تسميات عدة مرادفة، مثل **المهاجم** Attacker، و**المُعترِض** Interceptor، و**المُتطفِّل** Interloper، و**الدخيل** Intruder، و**المُناوِئ** Opponent، و**العدو** Enemy، و**المُتجسِّس** Tapper، و**المُتنصِّت أو المسترق** Eavesdropper.

أمّا **قناة التبادل** أو **قناة الاتصال** Communication Channel (واختصارًا تُدعَى فقط **القناة** Channel) فهي الوسيلة التي يَتم عبرها نَقْل المعلومات والرسائل من طرف إلى آخر، وتُشكِّل مجموعة قنوات الاتصال **الشبكة** Network. إنَّ أكبر وأشهر شبكة قنوات اتصال معروفة حاليًّا هي شبكة الإنترنت Internet، ولا تَفترِض التعمية أن تكون قناة الاتصال آمنة؛ لذا فهي تَعمَل، وتُؤدِّي دورها وفق ظروف القناة غير الآمنة، وإنَّ هذا الافتراض نابِع من افتراض المُرسِل والمُستقبِل الذي يَقضي بوجود الخصم في بيئة الاتصال التي يُشكِّلانها، حتى لو لم يكن هناك أصلًا.

في الشكل (1–3)، كَوْن قناة الاتصال تُعدّ قناة تبادل، فإنَّ المُرسِل هو مُستقبِل أحيانًا، والمُستقبِل هو مُرسِل أحيانًا، ولذا يَدُل الخط ذو الاتجاهين الواصل بين المُرسِل والمُستقبِل على ذلك، ويُشير الخط المنقَّط الذي يَصِل بين الخصم وقناة الاتصال إلى أنَّ الخصم هو طرف دخيل غير شرعي في قناة الاتصال. أمّا الاتجاهان المتعاكسان لهذا الخط المنقَّط فيَدُلّان على افتراض أنَّ الخصم يستطيع قراءة المعلومات المتبادَلة بين المُرسِل والمُستقبِل، وفي الوقت نفسه يستطيع التأثير فيها من خلال تعديلها.

الشكل (3_1) مخطط بيئة الاتصال الافتراضي