الفصل السادس

التعمية واستخراج المعمى أهم تقنيات أمن المعلومات[1]

(الشفرة وكسرها)

1.6 لمحة تاريخية.

يذكر علماء تاريخ هذه التقنية أن أنواعًا من سُبُل إخفاء المعلومات وسترها قد عرفتها الحضارة المصرية على ضفاف النيل في حدود عام 1900 قبل الميلاد، وتداولتها الحضارات الأخرى المجاورة.

واصطنع العرب في جاهليتهم الرمز، والملاحن، والمعاريض، وأمثالها؛ ليخفوا معانيهم ومراميهم، فلا يفهم عنهم إلاَّ الفَطِن ذو النباهة، فلما جاء الإسلام، واستبحر العمران، وازدهرت الحضارة العربية، وتشابكت مصالح الدولة التي امتدت أطرافها، وكثرت صلاتها بالدول الأخرى، تهيَّأت الأسبابُ المُسْعِفَةُ ليخطو العرب خطواتٍ فساحًا،

(1) بعض فقرات هذا الفصل مستقاة من مقالات للدكتور محمد مراياتي.

فيبدعوا في طرائق إخفاء أغراضهم ومقاصدهم، ويسلكوا في سبيل ذلك أساليب متنوعة مبتكرة، فيها الرمز، والألغاز، والملاحن، والتعمية، والمحاجاة، والتورية، وما إليها.

التعميةُ لغةً: الخفاءُ والالتباسُ، وهي في الاصطلاحِ: تحويلُ نصٍّ واضحٍ إلى آخرَ غيرِ مفهومٍ باستعمالِ طريقةٍ محدّدةٍ، يستطيعُ مَنْ يعرفُها أن يفهمَ النصَّ، واستخراجُها عكسُ ذلك، يجري فيه تحويلُ النصِّ المُعَمَّى إلى نصٍّ واضحٍ لِمَنْ لا يعرفُ مُسْبَقًا طريقةَ التعميةِ المستعملة[1].

إن علمَ التعميةِ واستخراجَ المعمى واحدٌ من علومٍ كثيرةٍ تدينُ للعربِ ولادةً ونشأةً وتطورًا، وهو ليس كغيرِه من العلوم التي ترجم العربُ بعضَ أصولِها، ثم أغنَوها، وطوّروها كالرياضياتِ والفيزياء والفلسفةِ، وإنما هو علمٌ عربيُّ المولدِ، يعودُ الفضلُ إلى العربِ في ابتكارِه، ووضعِ أُسُسِهِ، وإرساءِ قواعدِه، وتطويرِه إلى أن بلغ مرحلةً ناضجةً، وغدا ما وضعُوه فيه مرجعًا قبسَ منه المشتغلون بالتعميةِ من بعدُ، فالعربُ أوَّلُ من كتب في طرائقِ التعميةِ الرئيسةِ التي ما انفكَّ العالمُ يستخدمُ بعضَها حتى يومنا هذا، وهم أوَّلُ مَنْ وضع المنهجيّاتِ الأساسيةَ في علمِ استخراجِ المُعَمَّى، ودوَّنوا فيهما مصنَّفاتٍ مُسْتَقِلَّةً على غايةٍ من الأهميةِ منذ القرنِ الثالثِ الهجريِّ، وجُلُّها باقٍ في خزائنِ مكتباتِ العالمِ ينتظرُ مَنْ ينفضُ عنه غبارَ القرونِ، فسبقوا بذلك الغربيين نحوًا من سبعةِ قرونٍ، ومهَّدوا لهم، وتركوا بصماتٍ واضحةً في آثارهم، تشهدُ بفضلِ العربِ وريادتِهم.

كان للعرب والمسلمين مدارس في الفكر العلمي، منها ما اتبع مدارس قديمة، ومنها ما كان أصيلًا، فمن المدارس العربية الإسلامية الأصيلة مدرسة علماء الجبر، وعلماء المثلثات، ومدرسة علماء اللسانيات والصوتيات، ومدرسة علوم الإدارة وغيرها، وقد

---

(1) قال الزمخشري في (أساس البلاغة) (ت ع ب): «استخراج المُعَمَّى مَتْعَبَةٌ للخواطر». وإيراده هذا الكلام في مفتتح كلامه عن المادة يدل على ما يلاقيه المستخرج من تعب في حلّ التعمية، وعلى دقة في استخدام مصطلحي الاستخراج والمعمى.

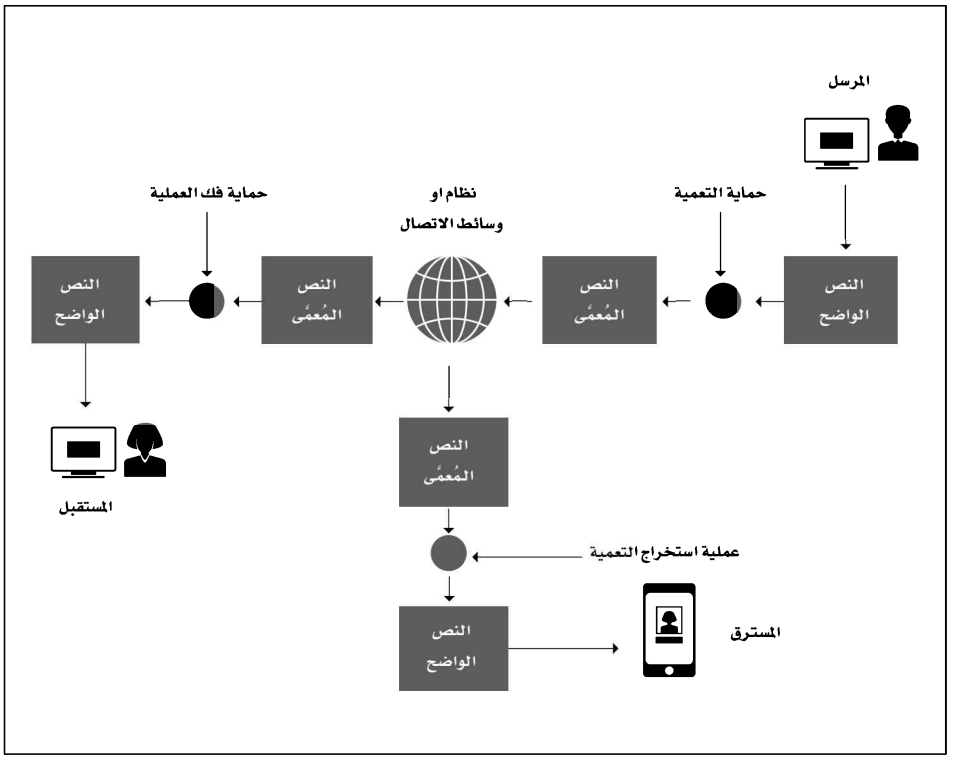
أضافت دراسة في جزأين، نشرت في 1200 صفحة من مجمع اللغة العربية بدمشق[1]، مدرسة علمية جديدة لم تكن معروفة قبلًا لطبيعة عملها، وهي المدرسة العربية في علوم التعمية (المعروفة الآن بعلوم الشفرة أو الكتابة السرية).

يعالج علم التعمية واستخراج المعمى مسألتين: تتناول الأولى طرق إخفاء المعلومات المرسلة من جهة إلى أخرى، وذلك لمنع المُسْتَرِق من الاطلاع على فحواها، وتتعلق الثانية باستخراج المعلومة من قبل المُسْتَرِق، وهذه المعركة بين المُعَمّي والمُستخرج قائمة سجالًا منذ أكثر من ألفي عام، فالأول يحاول ابتداع طريقة يَظُنُّ أنها لا تُستخرج، ويعمل الثاني جاهدًا على استخراجها، ويشارك في هذا التباري رياضيون، وفيزيائيون، ومعلوماتيون، ولغويون، وإلكترونيون، وغيرهم.

أخذ التخاطب عن بُعد أشكالًا مختلفة أهمها التراسل، وقد تطورت طرق التراسل ووسائلها مع الزمن لتأخذ حاليًّا أشكالًا مختلفة عدة، منها الرسائل البريدية، والتلكس، والبريد الإلكتروني، والتواصل عبر الجوالات، أو الهاتف المحمول بما في ذلك شبكات التواصل الاجتماعي وغيرها. أما وسائط التراسل فهي بريدية وسلكية ولاسلكية، وفي كثير من الأحيان يضطر الإنسان إلى إخفاء المعلومات التي يريد إرسالها إلى الطرف الآخر بهدف عدم اطلاع أي مُتطفل أو مُسْتَرِق على المعلومات المُرسلة، وهذه المعلومات قد تكون مهنية، أو تجارية، أو سياسية، أو دبلوماسية، أو عسكرية، أو... لذلك يقوم المُرْسِل بتعمية (تشفير) نص الرسالة قبل إرسالها للمُسْتَقْبِل الذي (يفكها) فور وصولها إليه لمعرفته بطريقة التعمية المتفق عليها مع المُرْسِل. أما المُسْتَرِق فيسعى إلى أخذ نسخة عن الرسالة خلال مسيرتها بين المتراسلين، ويحاول (استخراج تعميتها) على الرغم من عدم معرفته بطريقة التعمية المتفق عليها بين المُرْسِل والمُسْتَقْبِل، وهناك

(1) (التعمية واستخراج المعمى عند العرب) الجزء الأول والجزء الثاني، تأليف الدكاترة: محمد مراياتي، ويحيى مير علم، وحسان الطيان.

إذًا رغبة من قبل المتراسلين في تعقيد طريقة التعمية وجعلها مستحيلة (الاستخراج) يقابلها محاولة من المُسْتَرِق لنقض الطريقة واستخراجها؛ بغية الحصول على المعلومات المخفية فيها نظرًا لأهميتها، ويمثل الشكل مراحل عملية التواصل هذه:



عرفت التعميةُ في تاريخِها الطويلِ طرقًا عِدَّةً، يمكنُ إرجاعُ معظمِها إلى إحدى طريقتين هما:

أ. تعميةُ المعاني بالتوريةِ: هذه الطريقة لا تتبعُ قواعدَ محددةً، بل تعتمدُ على فطنةِ المتراسلينَ وخبرتهم وثقافتِهم(1)، وهي إلى العملِ الأدبيّ أو البديعي أقربُ منها إلى التعميةِ العلمية بمفهومِ هذا الكتاب، ولذلك سنتجاوز معالجةَ هذا اللونِ من المُعَمَّى على كثرةِ ما اجتمع من أصولِه الخطيةِ، ومن الأمثلة عليها: التورية،

والرمز، والألغاز، والملاحن، والمعاياة، والمحاجاة، وما إليها، فلن نتطرق لهذه الطرق في هذا الكتاب.

ب. التعميةُ بمعالجةِ الحروفِ: وتقومُ على اتِّباعِ طرقٍ تلتزمُ قواعدَ محددةً تخصُّ كُلًّا منها، وتدخل في منهجياتها مبادئ رياضياتية وخوارزميات معالجة محددة، وهذه الطرق هي المعنية بمعنى التعمية في هذا الكتاب.

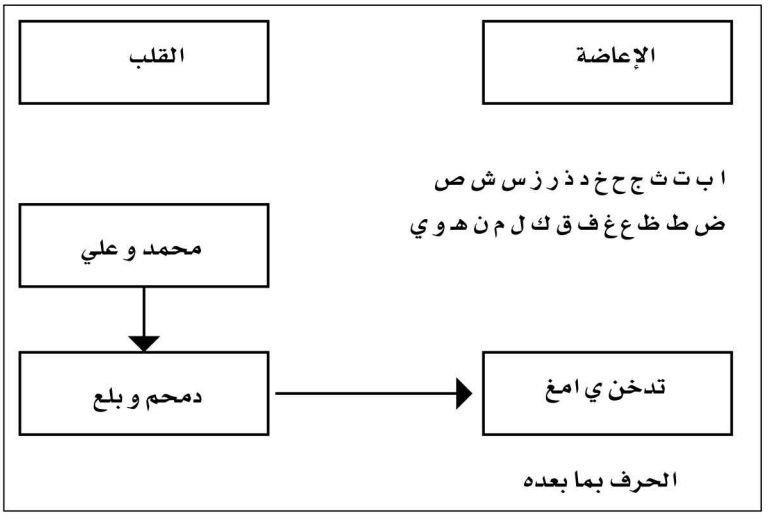
2.6 طرق التعمية الأساسية

أتينا سابقًا على التعاريف والمصطلحات الأساسية في علم التعمية واستخراج المعمى، ونتطرق في هذا الفصل إلى شرحٍ مبسطٍ وأمثلةٍ على الاستعمال والتطبيق.

تُقسَّم طرق التعمية التقليدية التي لم يُضَف إليها شيء جديد مهم حتى أوائل القرن العشرين، إلى أربعة أنواع، ذكرها الكندي واضع هذا العلم في مخطوطته، التي تُعدّ أول مرجع معروف في هذا العلم، وهي: التعمية بتبديل مواقع الحروف transposition، والتعمية بالإعاضة substitution، والتعمية بإضافة حروف (أغفال) nulls أو حذف حروف، ومثالُ ذلك أن تزيدَ حرفَ القافِ مثلًا بعد كلِّ ميمٍ، وحرفَ الشينِ بعد كلِّ لامٍ... إلخ، فَنُعَمِّي (محمد والد علي) على الشكلِ الآتي: (مقحمقد والشد علشي)، **والتعميةُ المركَّبةُ** Composite Cipher وتكونُ باستعمالِ طريقتينِ أو أكثرَ من الطرقِ الثلاثِ السابقةِ في آنٍ واحدٍ.

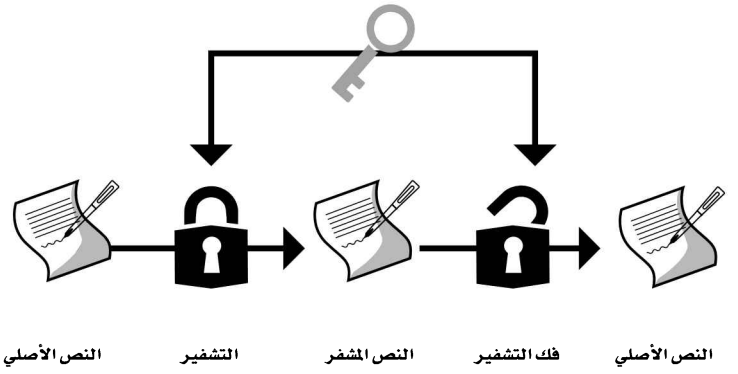
يبين الشكل الآتي شرحًا مبسطًا لعملية تعمية الكلمات: (**محمد وعلي**) باستعمال عمليتين متتاليتين: الأولى تغيير موقع الحروف في الكلمةTransposition كقلب المواقع مثلًا، حيث تصبح **محمد= دمحم**، وتصبح **علي = يلع**.

التعمية: تعريف ومثال

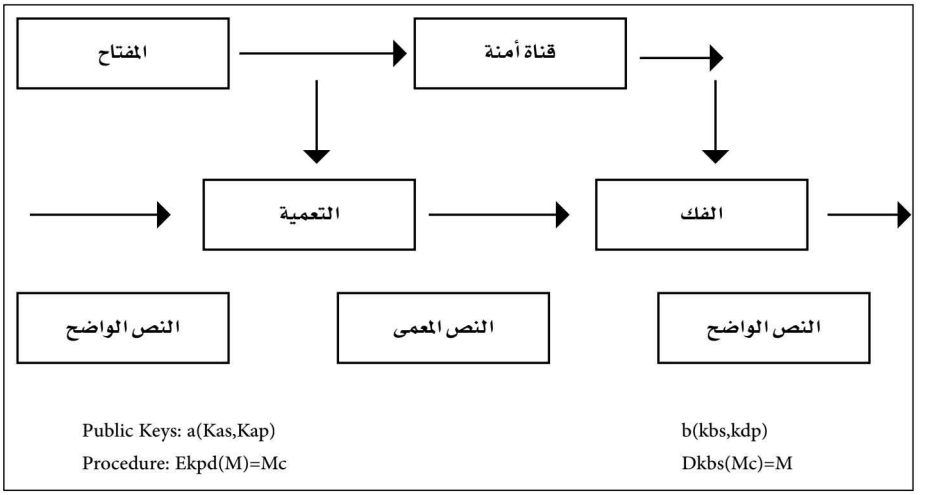


أما الطريقة الآتية فستكون باستعاضة شكل كل حرف بشكل حرف آخر ضمن الأبجديةSubstitution ، كأن يُستعاض عن الحرف بالحرف الذي يليه في الأبجدية: فتصبح **دمحم** = **ذنخن**، وتصبح **يلع** = **امغ**.

وتُقسَّم طرق التعمية إلى نوعين: متناظرة Symmetric وغير متناظرة Asymmetric، ففي التعمية المتناظرة يكون المفتاح المستعمل للتعمية المفتاح نفسه المستعمل لفك التعمية، ومن ثم فلا بد من إيجاد طريقة آمنة لإيصال المفتاح بين المتراسلين، ومن أمثلة التعمية المتناظرة نجد المعيار الأمريكي للتعمية DES وبعض مشابهاته.

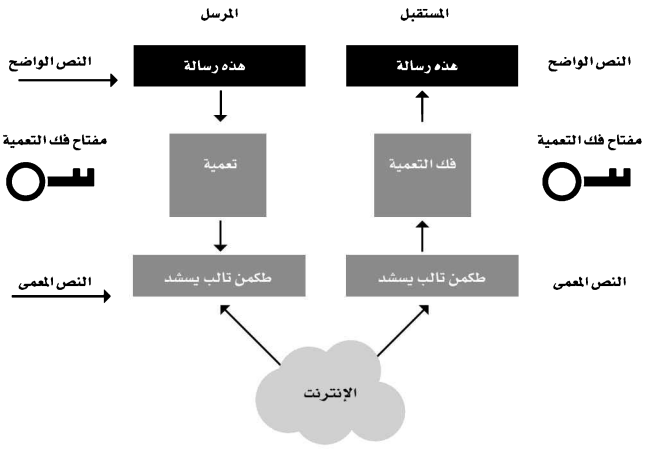


التعمية المتناظرة، التعمية بالمفتاح المعلن



أما في التعمية غير المتناظرة فيكون مفتاح التعمية مغايرًا لمفتاح فك التعمية، وتسمى هذه الطريقة أيضًا التعمية بالمفتاح المعلن Public Key؛ لأن لكل مراسل مفتاحين: أحدهما خاص وسري يحتفظ به لنفسه، والثاني معلن وفي متناول العامة، وعلى الرغم من وجود علاقة بين المفتاحين إلا أنه من غير الممكن عمليًّا حساب أحدهما لدى معرفة الآخر.

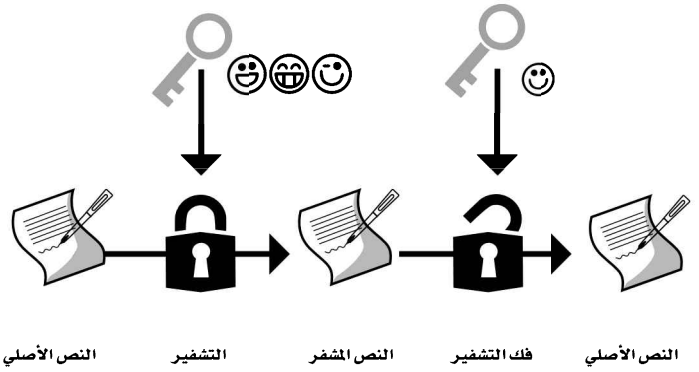
طريقة التعمية المتناظرة



من المألوف استعمال طريقتي التعمية معًا للاستفادة من ميزات كلٍّ منهما والإقلال من مساوئهما؛ لأن التعمية المتناظرة سريعة وآمنة أكثر من التعمية غير المتناظرة التي تحتاج إلى حسابات طويلة، وهي غير آمنة إذا كان مفتاحها قصيرًا، ومن جهة أخرى، فإن التعمية المتناظرة تحتاج إلى تبادل مسبق للمفتاح على عكس التعمية غير المتناظرة.

ويُستعمَل في معظم النظم العملية الموجودة في الأسواق التعمية بالمفتاح المعلن بهدف تبادل المفتاح السري اللازم للقيام باستعماله في التعمية المتناظرة، ويتم ذلك لكل مبادلة على الشبكة، ويسمى هذا المفتاح مفتاح جلسة المبادلة Session Key، وتجري تعمية المعلومات المتبادلة باستعمال التعمية المتناظرة ومفتاح الجلسة.

التعمية غير المتناظرة أو بالمفتاح المعلن



1.2.6 مبادئ وأمثلة في طرق التعمية المتناظرة الرئيسة:

ومن أهم طرق التعمية بالتبديل ما يكون بجمع حروف الرسالة، بعد ترميزها وفق نظام رقمي معين، جمعًا دائريًّا مع حروف مفتاح متفق عليه بين المتراسلين، فمثلًا إذا رمَّزنا حروف اللغة العربية بالأرقام العشرية من /1/ إلى /28/ بحسب ترتيب أبجد، وكان المفتاح المتفق عليه هو: (كليلة ودمنة) = B، تكون عملية التعمية بهذه الطريقة وفق ما يأتي:

- The clear message M, the encrypted message E(M), and the two keys (Ks,Kp) are represented by positive integers numbers.
- The keys are generated

n=q*p r=(q-1)(p-1) 77=11*7 60=(11-1)(7-1)

e<r e&r have no common divider e=37 or 11,19 etc

e*d=1 mod (r) 37d=1 mod(60) d=13

Ks=(d,n) Kp=(e,n) Ks=(13,77) Kp=(37,77)

- It is difficult to find d knowing n and e if q and p are of 100 digits.
- E(M)=M**e mod(n)
- M=E(M)**d

نظام ترميز عشري													
أ	ب	ج	د	ه	و	ز	ح	ط	ي	ك	ل	م	ن
1	2	3	4	5	6	7	8	9	10	11	12	13	14
س	ع	ف	ص	ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
15	16	17	18	19	20	21	22	23	24	25	26	27	28

ولتكن الرسالة المُراد تعميتها هي: (يكثف العمل صباح الغد) = A

الرسالة الواضحة A	ي	ك	ث	ف	ا	ل	ع	م	ص	ب	ا	ح	ا	ل	غ	د
المفتاح B	ك	ل	ي	ل	هـ	و	د	م	هـ	ك	ل	ي	ل	هـ	و	د
ترميز الرسالة الواضحة	10	11	23	17	1	12	16	13	18	2	1	3	1	12	28	4
ترميز المفتاح	11	12	10	12	5	6	4	13	5	11	12	10	12	5	6	4
ترميز الرسالة المعمّاة بالجمع الدائري	21	23	5	1	6	18	20	26	23	13	13	13	13	17	6	8
الرسالة المعماة C	ش	ث	هـ	ا	و	ص	ر	ض	ض	ث	م	م	م	ف	و	ح

مثال على الجمع الدائري بأساس 28 «إذا تجاوزت النتيجة 28 فيطرح منها 28»:

$1 = 17 + 12$ $\quad$ $6 = 28 + 6$ $\quad$ $5 = 23 + 10$

فيكون النص المُعَمَّى هو: | C = (شثها وصرضض ثممم مفوح) |

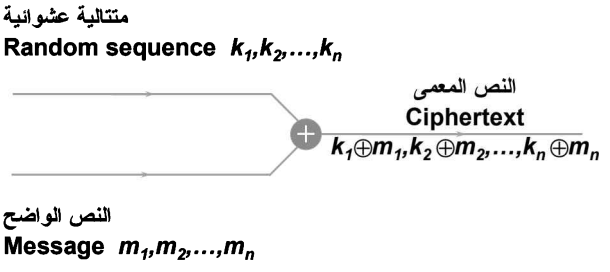
وبهذا، فعملية التعمية التي يقوم بها المُرْسِل هي الآتية:

$$C = A \rho B$$

حيث A هي النص الواضح وB هي المفتاح وC هي النص المُعَمَّى، أما المُسْتَقْبِل الذي يعرف المفتاح فيقوم بالعملية الآتية:

$$A = C \sigma B$$

تعمية فيرمان Vernam Cipher



كلا الرسالة والمفتاح متتالية من الخانات الإثنانية
The message and key are bit strings

حيث r هي عملية الجمع الدائري بالقياس /28/: modulo 28 وs عملية الطرح، أما المُسْتَرِق فسيحاول استخراج التعمية عن طريق اكتشاف المفتاح المستعمل، وهذا ممكن إذا كانت الرسالة أطول من المفتاح بمرات عدة، وهي أسهل إذا كان المفتاح جملة مفيدة.

واقترح فيرنام Gilbert Vernam عام 1917م، خلال الحرب العالمية الأولى، استعمال مفتاح عشوائي غير ذي معنى، طوله يساوي طول النص الواضح، وقد أُثبت رياضياتيًّا عام 1948م أن هذه الطريقة غير قابلة للاستخراج، وبهذا تكون منظومة التعمية هذه هي الوحيدة التي أُثبت رياضياتيًّا أنها آمنة، شريطة عدم استعمال المفتاح نفسه أكثر من مرة واحدة، وعدم حصول المُسْتَرِق على المفتاح بطرق أخرى، وتكون المفاتيح في سِجلّ، تحوي كل صفحة منه مفتاحًا، وتستعمل الصفحة مرة واحدة تتلف بعدها، ومن هنا أتت تسمية الطريقة بـ (سِجلّ المرة الواحدة) one time pad، ويمكن أن نفهم بسهولة سبب استحالة استخراج هذه التعمية لمن لا يعرف المفتاح مما يأتي: إن النص الذي ستعميه يمكن أن ينتج عنه أي نص، وذلك بحسب المفتاح الذي تستخدمه، فيمكن لكلمة (محمد) أن تعطي بحسب المفتاح، على حد سواء، كلمة (حشلم) أو كلمة (شخشك) أو كلمة (سامر) أو أي كلمة ذات أربعة حروف، ولذلك كان من المستحيل على من لا يعرف المفتاح نفسه أن يستخرج كلمة (محمد) الأصلية، ولهذه الخاصية استخدمت طريقة التعمية هذه في (الهاتف الأحمر) بين موسكو وواشنطن، الذي قيل فيه: إن أشرطة تسجيل مغناطيسية، محروسة بعناية، تنقل باستمرار بين واشنطن وموسكو بالطائرة.

لذا كانت سيئة نظام تعمية فيرنام أو نظام (سِجلّ المرة الواحدة) في ضرورة توزيع سِجلّ المفاتيح بين المتراسلين مسبقًا، وهذه عملية صعبة ومكلفة وغير آمنة، فهي أولًا صعبة أو مكلفة؛ لأنه يجب إرسال سِجلّ المفاتيح لكل المستقبلين قبل التراسل، على أن تكون هذه السجلات مختلفة عن بعضها، ويجب حفظها لدى المُسْتَقْبِل طوال مدة التراسل، وهي ثانيًا غير آمنة؛ لأن هناك احتمال استراق سِجلّ المفاتيح خلال عملية التوزيع أو خلال مدة الحفظ لدى المُسْتَقْبِل، وعملية التوزيع هي عن طريق المراسل أو البريد أو الوسائط السلكية أو اللاسلكية، وهي كلها عُرضة للاستراق، وحفظها مدة من

الزمن لدى المُسْتَقْبِل قبل استعمالها يعرضها أيضًا للاستراق، وهنا يأتي ميكانيك الكم ليحل هذه المشكلة، ويضمن توزيع المفاتيح العشوائية بأمان تام كما سنرى.

لنستعمل الآن نظام ترميز اثناني بدل النظام العشري، كما هو مبين في الجدول الآتي:

نظام ترميز اثناني						
2^4	2^3	2^2	2^1	2^0	الحرف	الرمز العشري
0	0	0	0	1	أ	1
0	0	0	1	0	ب	2
0	0	0	1	1	ج	3
0	0	1	0	0	د	4
0	0	1	0	1	ه	5
0	0	1	1	0	و	6
0	0	1	1	1	ز	7
0	1	0	0	0	ح	8
0	1	0	0	1	ط	9
0	1	0	1	0	ي	10
0	1	0	1	1	ك	11
0	1	1	0	0	ل	12
0	1	1	0	1	م	13
0	1	1	1	0	ن	14
0	1	1	1	1	س	15
1	0	0	0	0	ع	16
1	0	0	0	1	ف	17
1	0	0	1	0	ص	18
1	0	0	1	1	ق	19
1	0	1	0	0	ر	20
1	0	1	0	1	ش	21
1	0	1	1	0	ت	22
1	0	1	1	1	ث	23
1	1	0	0	0	خ	24
1	1	0	0	1	ذ	25
1	1	0	1	0	ض	26
1	1	0	1	1	ظ	27
1	1	1	0	0	غ	28

الجمع الدائري

$0 \rho 0 = 0$ $\quad$ $1 \rho 1 = 0$

$0 \rho 1 = 1$ $\quad$ $1 \rho 0 = 1$

ليكن النص الواضح هو (محمد) فترميزه وفق النظام الاثناني (01101 – 01000 – 01101 – 00100) = A فإذا كان المفتاح متتالية عشوائية اثنانية، طولها طول المفتاح (0010110101000110101 1) =B، وكان الجمع الدائري في الحقل /2/ (modulo 2).

تكون عملية التعمية كما يأتي: C = A ρ B ويبعث المُرْسِل C للمستقبل.

النص الواضح	م	ح	م	د
ترميز النص الواضح A	01101	01000	01101	00100
ترميز المفتاح B	010011	00011	10101	00101
ترميز الرسالة المعماة بالجمع الدائري C	00110	01011	11000	00001
الرسالة المعماة	و	ك	خ	ا

فإذا جمع المُسْتَقْبِل جمعًا دائريًّا C مع B فيحصل على النص الأصلي A وتبقى المسألة هنا هي توزيع سِجلّ المفاتيح، وهو متتالية عشوائية اثنانية آمنة بين المتراسلين، ومن ثم نصل إلى الهدف المنشود في نظام غير قابل للاستخراج، وهنا يأتي ميكانيك الكم ليقدم الحل لهذه المشكلة، وهو يكمن في قناة اتصال محمية من كل استراق يستحيل تجسسها دون شعور المتراسلين بذلك، حيث تكون الفوتونات المستقطبة حاملة للمعلومة (1) أو (0) بحسب استقطاب الفوتون.

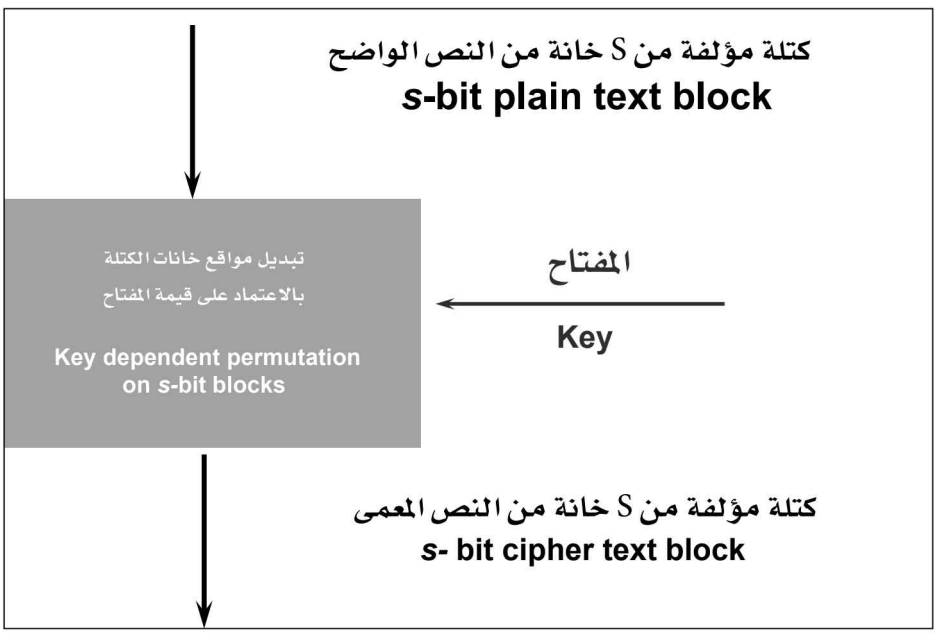
وقد حقق ميكانيك الكم أخيرًا تقدمًا عظيمًا في هذا الاتجاه لم يستطع الرياضياتيّون وحدهم تحقيقه، وتستخدم وسائل التعمية الكمومية فوتونات ضوئية إفرادية، وتعتمد على مبدأ هايزنبرك في الارتياب لتحقيق هدفها في التعمية غير القابلة للاستخراج، بل إن مجرد الاستراق يصبح غير ممكن دون تنبيه المتراسلين، وتسمح تقنية التعمية الكمومية أيضًا بتحقيق عمليات أخرى، مثل التحقق من هوية المُرْسِل، ومثل فكرة الأوراق النقدية غير القابلة للتزوير، وغيرها. والجدير بالذكر أن شركة IBM قد طرحت للعامة

حاسوب كمومي أوليًّا في إبريل من عام 2016م يمكن تجربته عن طريق موقعها على الإنترنت في مثل التعمية الكمومية[1].

وتتميز التعمية الكمومية بأنها تعتمد مبدأ (سِجلّ المرة الواحدة) وهو غير قابل للاستخراج، وتحقق نقل المفتاح العشوائي بين المتراسلين بأمان؛ لأنها تنبه المتراسلين إلى وجود مسترق عند حدوث الاستراق.

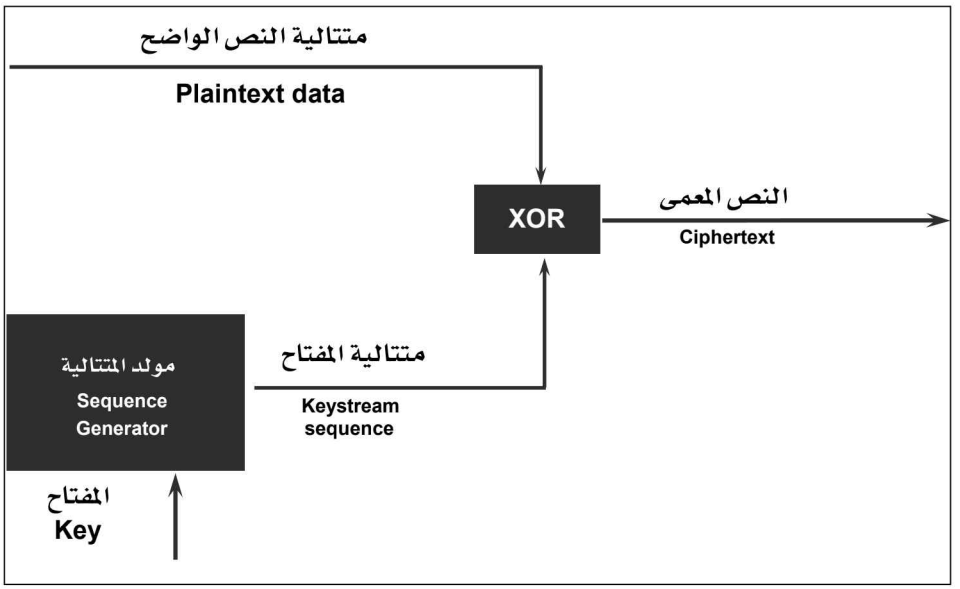
وتجدر الإشارة إلى أن التعمية المتناظرة الحديثة تستخدم نظامين من أنظمة التعمية، وهما التعمية التسلسلية stream cipher والتعمية الكتلوية block cipher، ويبين الشكلان الآتيان شرحًا لهذين النظامين، وفي كلا النظامين تكون الرسالة والمفتاح مرمزتين اثنانيًّا؛ أي باستعمال (1) و(0).

نظام تعمية كتلوي متناظر Symmetric Block Cipher System



(1) جريدة الرياض، الأربعاء 04 شعبان 1437هـ/ 11 مايو 2016م.

التعمية التسلسلية (متتالية إثنانية) Stream Cipher



2.2.6 الوسائل والعلوم المستخدمة في التعمية واستخراجها

إن الوسائل التي كانت مستخدمة في علوم التعمية في القرون الوسطى هي الورق، والقلم، والخرز الملون، وعقد الأصابع، وشبكات الاتصالات البريدية، وغيرها، أما الآن فلا يزال الورق والقلم مستعملًا إلا أن الأجهزة الميكانيكية (المسننات) طغت في أواسط القرن العشرين، أما الأجهزة الإلكترونية والحواسيب وشبكات الاتصال الإلكترونية، فأصبحت هي الغالبة الآن.

وتقع أسس علوم التعمية في مجالات متعددة أهمها الرياضية، مثل علم الأرقام، وعلم الإحصاء والاحتمالات، والجبر البولي، ونظرية التعقيد، ومعالجة الإشارة، ونظرية الألعاب، وغيرها، وتليها الأسس اللسانية من علوم الصوتيات، والصرف، والنحو، والدلالة، واللسانيات الحاسوبية، يضاف إليها أيضًا علوم الإدارة، وعلوم الإلكترونيات، والمعلوميات، وميكانيك الكم.

3.6 طول المفتاح وقوة التشفير.

تُعدّ عملية توليد المفاتيح أكثر العمليات حساسية في التعمية، فحتى يكون نظام التعمية سريًّا قدر الإمكان يجب أن تكون المفاتيح أعدادًا عشوائية حقًّا وغير قابلة للتنبؤ من قِبَل مستخرجي التعمية، إن مثل هذه الأعداد المطلوبة تختلف عن تلك التي تولدها الحواسيب خوارزميًّا باستعمال المتتاليات المحدودة شبه العشوائية من أجل استخدامها في الألعاب وفي عمليات تمثيل النظم الطبيعية Simulations، إذ إن الأعداد العشوائية حقًّا لا يمكن استخراجها إلا من (الضجيج) البيئي لعالمنا الفيزيائي، لكن توليد مثل هذه الأعداد العشوائية عالية الجودة في الحاسوب أمر صعب.

ومن المفيد ملاحظة أن نظام التعمية الوحيد الذي أثبت علماء التعمية سريته التامة، هو ما يسمى (سِجلّ المرة الواحدة) (OTP) One Time Pad الذي يكون فيه طول المفتاح العشوائي مساويًا لطول الرسالة نفسها، ففي هذا النظام تستخدم سلسلة عشوائية لتعمية الرسالة خانة خانة (Bit for Bit) أي إن الخانة (Bit) الرابعة والثلاثين من المفتاح تُستخدَم لتغيير الخانة الرابعة والثلاثين من الرسالة، والمفتاح يجب أن يكون عشوائيًّا حقًّا، فلا يقبل أن يكون سلسلة شبه عشوائية مولدة عن طريق خوارزمية محددة؛ لأنه عندها ستكون التعمية قابلة للكسر، ولكن نادرًا ما يجري استخدم نظم التعمية بـ (سِجل المرة الواحدة) OTP؛ لأنها غير عملية، إذ يجب على المفتاح أن يكون بطول الرسالة، ويجب إرساله للمستقبل عبر قناة سرية، والأنكى من ذلك أنه يستعمل مرة واحدة، وإلا فهو معرّض للاستخراج.

وعلى الرغم من اعتقاد كثير من الناس أن طول المفتاح هو العامل الحاسم في قوة التعمية، إلا أن هناك صفة لا تقل أهمية ألا وهي جودة تصميم نظام التعمية، ولنأخذ على سبيل المثال التعمية بالإعاضة البسيطة التي يُستعاض فيها مثلًا عن كل الألفات

بالسينات، وكل الباءات بالكافات، وكل التاءات بالفاءات، وهكذا... إن عدد الطرق هذه التي يمكن بها ترتيب الألفبائية العربية المؤلفة من 28 حرفًا يُعطى بالعلاقة:

28! (أي 1x2x3x 4x5x.....x26x27x28)، هذه الكمية تساوي (0488, 3 ×10 29) وهذا العدد من المفاتيح الممكنة يُعدّ (فضاء مفتاح) مقبولًا نسبيًّا، ويتطلب معدات حاسوبية ضخمة لكسره إذا أردنا فحص كل المفاتيح الممكنة حتى الوصول إلى النص الواضح، إلا أنه يمكن استخراج هذا النوع من التعمية دائمًا دون الحاجة لأكثر من ورقة وقلم رصاص، ويكون ذلك بأن نتفقد ببساطة الحرف الأكثر تواترًا في النص المعمى وافتراضه ألفًا (في حال اللغة العربية) وبعدها نتفقد الحرف الثاني الأكثر تواترًا، ونفترضه لامًا، وهكذا حتى نستخرج التعمية. إذًا، فعلى الرغم من أن (فضاء المفتاح) في هذه الطريقة كبير إلا أن الطريقة ضعيفة للغاية.

والحقيقة أن نظم التعمية ذات التصميم الجيد تحتاج في كسرها إلى جهد يتناسب مع طول المفتاح، ففي حالة التعمية الكتلوية (أو المقطعية) Block cipher تكون هذه العلاقة أسية، فعندما نزيد طول المفتاح خانة واحدة (1 Bit) يتضاعف عمل المستخرج في تجربته جميع المفاتيح الممكنة، وعندما نضاعف طول المفتاح، فيجب أن نربع كمية الجهد المطلوب، فمن أجل مفتاح طوله 128Bit نحتاج وسطيًّا إلى 2128 (7, 1 1038 x) عملية حسابية لاستخراج هذه التعمية.

ومن جهة أخرى تكون خوارزميات التعمية بالمفتاح المعلن أقل حساسية لطول المفتاح، فعادةً يكون فضاء المفاتيح تحت أسي، ولكن فوق خطي، وهذا يعني أن مضاعفة طول المفتاح يزيد كمية الجهد المطلوب لاستخراج التعمية كثيرًا، إلا أن هذه الكمية هي أقل من مربع الجهد، فإذا استعملنا خوارزمية التعمية بالمفتاح المعلنRSA على سبيل المثال نجد أن الخوارزميات الحديثة للتحليل إلى العوامل الأولية لا تعتمد تجربة كل الأعداد الأولية الأصغر الممكنة للوصول إلى تحليل العدد، بل تستعمل طرقًا أكثر جدوى

بكثير، وكذلك فطريقة ديفي- هلمان هي تحت أسية، وبغية إعطاء فكرة للمقارنة بين التعمية غير المتناظرة وتلك المتناظرة، فإن التعمية بمفتاح طوله3000 Bit بطريقة RSA أو ديفي- هلمان تطلب لاستخراجها تقريبًا الكمية نفسها من الجهد الذي تتطلبه طريقة التعمية المقطعية ذات مفتاح بطول 128 Bit.

التعمية المقطعية صعبة المنال نسبيًا على المستخرجين، وعلى الرغم من ذلك، فقد قامت شركة Electric Frontier Foundation منذ 20 عامًا ببناء حاسوب تفرعي خاص (أي مجموعة من الحواسيب تعمل على التوازي) أمكنه استخراج تعمية رسالة مشفرة بخوارزمية DES بمدة حساب تقل عن أسبوع، وذلك عن طريق تجريب كل المفاتيح الممكنة لفضاء مفتاح بطول 56 خانة Bit 56 .

إن استخراج المعمى بطريقة تجريب المفاتيح جميعها (طريقة القوى العمياء) ليست الطريقة الوحيدة، فأهل هذا العلم يستطيعون استخدام أدوات إحصائية ورياضياتية قوية لإيجاد طرق مختصرة ككشف بعض تراكيب النص المعمى، ويمكن تبويب طرق استخراج المعمى في ثلاثة أنواع، وذلك تبعًا لمدى معرفتنا لمعلومات عن النص الواضح والنص المشفر المقابل له.

ففي بعض الحالات يكون كل ما يعرفه المستخرج هو النص المعمى فقط، ومن ثم يكون لديه القليل من المعلومات التي يمكن أن تساعده على تخمين المفتاح، وفي هذه الحالة يمكن حتى لطرق التعمية سيئة التصميم أن تصمد أمام الهجوم بمعرفة النص المشفر فقط، ولكن إذا وصل إلى علم المستخرج على الأقل جزء من النص الواضح، مثلًا أن النص يبدأ بجملة: (عزيزي السيد سامر) فإن فرص النجاح تزداد بشكل كبير، فعلى الأقل يمكن للمستخرج أن يجرب عددًا من المفاتيح المختلفة حتى يصل إلى مفتاح منها يفك به تعمية (عزيزي السيد سامر) حتى إذا عرف المستخرج لغة النص الواضح فقط (مثلًا الروسية أو الفرنسية أو العربية) فإن هذه المعلومة ستساعده كثيرًا، فإذا

كانت الرسالة بالإنجليزية فالمعروف أن أكثر الكلمات تواترًا هي «The» من أجل هذا وبغية الحماية من استخراج التعمية بالكلمة المحتملة تقوم بعض نظم التعمية بالضغط الإلكتروني للرسالة قبل تعميتها بهدف إخفاء التراكيب التي يسهل التنبؤ بها.

يعرف المستخرج عادةً معلومات تزيد عما ذكرناه أعلاه، فإذا قام أحدهم بسرقة (بطاقة ذكية) تحتوي على دارات تعمية، فإنه ربما يستطيع تجريب بلايين الرسائل المنتقاة بدقة لهذه البطاقة ثم دراسة النصوص المعماة الناتجة، فمثل هذه الطريقة في الاستخراج باستعمال نصوص واضحة منتقاة يمكنها أن تكسر بسهولة نظام تعمية سيئ التصميم، ولنضرب مثالًا آخر حول نظام المفتاح المعلن، إذ يمكن للمستخرج أن يكتب رسالة، ثم يقوم بتعميتها بالمفتاح المعلن (المتاح للجميع) وبعدها يقوم بتحليل النص المعمى الناتج.

لقد جرى تطوير طريقتين فعالتين جدًّا في استخراج المعمى ألا وهما طريقة الفروق (أو الطريقة التفاضلية) والطريقة الخطية، وقد استعمل كلا المنهجين لكسر عدد من طرق التعمية المعروفة، وكذلك للبرهنة على إمكانية كسر معيار التعمية DES بسرعة تفوق بمئات بل آلاف المرات عن تلك التي تقوم على تجربة جميع المفاتيح الممكنة.

إن طريقة الاستخراج بالفروق تعتمد على تعمية عدد كبير من أزواج النصوص الواضحة ذات الفروق المنتقاة بدقة من أجل إيجاد أزواج النصوص المعماة المقابلة التي تتمتع بعدم تشابه محدد، فعند الوصول إلى زوج من هذه الأزواج، فإنه ستُكشَف للمستخرج معلومات حول المفتاح المستخدم، أما في طريقة الاستخراج الخطية والمطورة في شركة ميتسوبيشي اليابانية فيجري البحث عن الترابط بين النص الواضح والنص المعمى والمفتاح الموجودة أكثر مما يتوقع، ثم القيام بعد ذلك بإجراء إحصائيات على عدد كبير من الأزواج، نص واضح – نص معمى، وذلك بهدف إيجاد انحيازات تكشف معلومات عن المفتاح.

4.6 أمان خوارزميات التعمية

ثمة ثلاثة مداخل رئيسة لقياس أمان خوارزميات التعمية:

- إذا كانت التكلفة المالية المطلوبة لكَسر الخوارزمية أكبر من القيمة الفعلية التي تَحمِلها المعلومات المُعمَّاة فهي آمنة.
- إذا كانت المدة (الزمن) المطلوبة لكَسِر الخوارزمية أكبر من المدة التي يَنبغي أن تكون المعلومات في غضونها محمية (مُعمَّاة) فهي آمنة.
- إذا كان مقدار المعلومات المطلوبة لكَسِر الخوارزمية أكبر من مقدار المعلومات المُعمَّاة فهي آمنة. (المعلومات التي قد تكون ضرورية لكَسِر خوارزمية التعمية تَتمثَّل مثلًا في تفاصيل دقيقة عن الخوارزمية، ونتائج لهجمات تمَّت مسبقًا، وتحليلات ضخمة لعمل الخوارزمية، و... إلخ).

عمومًا، يجب أن تُبنَى خوارزمية التعمية، بحيث يَنبغي أن تَبقى المعلومات المحمية بها (مهما كان مستوى حساسيتها) أقل قيمة من تكلفة كسرها.

1.5.6 نماذج تقييم أمان خوارزميات التعمية

يمكننا تقييم أمان خوارزميات التعمية من خلال تصنيفها إلى نموذجين أساسيين: **خوارزميات آمنة بلا قيد** Unconditionally Secure Algorithms، و**خوارزميات آمنة حسابيًّا** Algorithms Computationally Secure.

الخوارزمية الآمنة بلا قيد.

تُعدّ خوارزمية التعمية آمنة بلا قيد إذا لم تتوافر معلومات كافية لاستعادة النص الواضح من نص معمّى مقابل، ويُفتَرَض في الخصم، في نطاق هذا النموذج، أن يمتلك موارد حسابية (وغير حسابية، زمن كافٍ - راحة - مال - ...) غير محدودة من أجل أن يشن هجومًا على الخوارزمية لكسرها، ولكن يظل مع كل تلك الموارد غير قادر على

استعادة النص الواضح، وإنَّ أمان هذه الخوارزميات هو أمان مطلق (غير مشروط)؛ لذا تُسمّى السريّة التي تقدّمها **السريّة المثالية** Perfect Secrecy. إنَّ مستوى السريّة المثالية هو هدف لكل مصمم خطة تعمية، وليس ثمّة خوارزمية تعمية تستطيع أن تحقق مثل هذا الأمن المطلق إلا خوارزمية (سِجلّ المرة الواحدة) one–time pad.

ثمّة شرطان أساسيان ليكون نظام التعمية المتماثل آمنًا بلا قيد: الأول، أن يكون المفتاح عشوائيًّا تمامًا، وأن يكون طوله مساويًا على الأقل لطول الرسالة، وألا يُستخدَم مرة ثانية، والثاني، ألا تتوافر المعلومات اللازمة للتيقّن من حقيقة النص الواضح المسترجع بعد كسر تعمية النص المعمّى المقابل؛ أي يجب أن يتوافر عدد كبير من النصوص الواضحة المقبولة بوصفها حلولًا للنص المعمّى، بحيث لا توجد طريقة لتحديد النص الواضح الأصلي الحقيقي من بين تلك النصوص الواضحة المسترجعة.

وكما قلنا: إنَّ نظام (سِجلّ المرة الواحدة) هو أكبر مثال عن خوارزمية تعمية متماثلة آمنة بلا قيد، أمَّا بقية خوارزميات التعمية المتماثلة فلا تقدّم الأمان المطلق، إذ إنها من النموذج الثاني.

بالنسبة إلى خطط التعمية بالمفتاح العلني فهي بالتأكيد لا تقدّم الأمان المطلق، والسبب هو: بتوافر النص المعمّى $c \in C$ والمفتاح العلني $e \in K$، يمكن استرجاع النص الواضح $m \in M$ عن طريق تعمية جميع عناصر فضاء النص الواضح M بالمفتاح e ومقارنة النتائج بالنص المعمّى الموجود، وإذا تطابقت نتيجة تعمية أحد النصوص الواضحة m بالمفتاح e مع نص معمّى c فذلك هو المطلوب (دون الحاجة إلى اكتشاف المفتاح الخاص $d \in K$).

الخوارزمية الآمنة حسابيًّا.

تُعدّ الخوارزمية آمنة حسابيًّا، وتُدعى حينها **الخوارزمية القويّة** Strong Algorithm، إذا تعذر كسرها مع وجود الموارد الحسابية الآنية على الأقل أو المستقبلية، وإنَّ جميع

خوارزميات وأنظمة التعمية الحالية المتماثلة وغير المتماثلة (ماعدا نظام: سِجلّ المرة الواحدة one–time pad) هي أمثلة عن نموذج الخوارزمية الآمنة حسابيًّا، وعمومًا تهتم تقنيات التعمية الحديثة، وتركّز على هذا النموذج فقط.

تتصف خوارزمية التعمية بأنها **قابلة للكسر** Breakable إذا استطاع طرفٌ[1] ما أن يكتشف، أو أن يصوغ طريقة لاستعادة النص الواضح من النص المعمّى المقابل دون معرفة ولو جزئية بالزوج المفتاحي (e، d) في إطار زمني معيّن، ويتحدد الإطار الزمني بالمدة التي تصغر المدة التي تكون في غضونها المعلومات المعمّاة ذات أهمية، وإنَّ هذا الإطار الزمني هو تابع لعمر أهمية المعلومات المحمية التي تحمل قيمة ما، وعلى سبيل المثال، لو تم التخطيط لدى قيادة جيش في بلدٍ ما لشن حرب على بلدٍ آخر في وقت معيّن، ووجبَ أن تكون هذه المعلومات سريّة (معمّاة) إلى وقت تنفيذ الهجوم؛ أي لنقل: 48 ساعة، فإنَّ عمر أهمية هذه المعلومات هو 48 ساعة بالتمام، ولن يستفيد الخصم، بعد اعتراضه وحصوله على هذه المعلومات المعمّاة، من معرفة مضمونها ومحتواها حتى ولو بعد ثانية من مرور الـ 48 ساعة؛ لأنَّ هذه المعلومات تكون قد فقدت أهميتها، والإطار الزمني لكسر حماية تلك المعلومات يتحدد بين 1 ثانية و47،59،59 ثا/ د/ سا.

ينبغي أن تُصمَّم خوارزميات التعمية الحديثة، بحيث تكون غير **قابلة للكسر** Unbreakable مع توافر الموارد الحسابية الآنية المتوقّع أن تزداد، وتتضاعف في المستقبل القريب.

تزداد الثقة في أمن خوارزمية التعمية إذا ما تصدَّت وبشكل دائم لعمليات التحليل المختلفة التي يقوم بها خبراء كبار في علم تحليل التعمية، وإنَّ مثل الخوارزميات التي يمضي عليها سنوات، ولم تنجح أي عملية تحليل لاختراق أمنها تُعدّ أفضل من تلك

(1) قد يكون هذا الطرف خصمًا، وقد يكون مصمم الخوارزمية نفسه الذي يقوم بهذا العمل بهدف اكتشاف نقاط الضعف.

الخوارزميات الحديثة التي يُعلن مصمموها أنها الأفضل، وأنها تقدّم أمنًا أكثر، ولا يمكن أن تُكسَر.

ينص الافتراض الأساسي في التعمية على أن تكون فضاءات النص الواضح M والنص المعمّى C والمفتاح K ومجموعة توابع التعمية $\{Ee: e \in K\}$ وتوابع فك التعمية $\{Dd: d \in K\}$ معروفة للجميع دون استثناء، لكنَّ الشيئين اللذين يجب على طرفي الاتصال الاحتفاظ بهما سرًّا هما النص الواضح m والزوج المفتاحي (e, d)[1]، وما يخالف هذا الافتراض هو التفكير في وجوب اعتماد أمان الخوارزمية على جعل الطريقة التي تعمل بها سرًّا، وتُدعى مثل هذه الخوارزمية **الخوارزمية المقيَّدة** Restricted algorithm.

مما لا شك فيه، فإنه لا أحد يستخدم الخوارزميات المقيّدة في هذه الأيام، إذ إنها غير كفأة لمقاييس الحماية المطلوبة للمعلومات السريّة، ومع ذلك تبقى مستعملة داخل كثير من التطبيقات المنخفضة السريّة لأغراض تتصف فيها حماية المعلومات بأنها مجرد أداة ثانوية ملحقة، ومن الصعب جدًّا استعمال الخوارزميات المقيّدة في تراسل المعطيات المحمية عبر الشبكة؛ لأن ذلك يتطلب إعداد شبكات اتصال خاصة لنقل تلك الخوارزميات بأمان إلى الأطراف الأخرى، ومن صفات الخوارزميات المقيّدة أنها لا تخضع لبحوث تحليلية، وهي على الأغلب للاستخدام الشخصي فقط.

ولقد تَعرَّف المجتمع التعموي الحديث منذ نشوئه إلى مجموعة من المبادئ الأساسية لبناء أي خطة تعمية، وسُميّت هذه المبادئ **مبادئ** Kerckhoffs، وأصبحت افتراضات ومتطلبات في الوقت نفسه لأي نظام تعمية، ونصَّ أحد تلك المبادئ على إرشاد يخالف استعمال الخوارزميات المقيّدة، حيث دعا إلى أن تكون تفاصيل الخوارزمية علنية وصريحة وغير سريّة.

---

(1) إذا كان $e = d$ فيجب الاحتفاظ بهما معًا؛ كونهما تركيبة واحدة، وإذا كان $e \neq d$ فيجب الاحتفاظ بالمفتاح d فقط، أمّا المفتاح e فينبغي أن يكون علنيًّا.

2.5.6 مبادئ Kerckhoffs في أمان خوارزمية التعمية

نَشَر عالِم اللغة وخبير التعمية البروفيسور الهولندي Auguste Kerckhoffs عام 1883م مقالة بعنوان (La Cryptographie Militaire) باللغة الفرنسية، التي تعني (التعمية العسكرية)، احتوت على ستة مبادئ أساسية لبناء خطط التعمية العكسرية، ولكن بسبب تحقيقها لمعظم مقاييس أمن المعلومات، تم تعميمها لتشمل خطط التعمية المدنية، وبسبب تغيّر الظروف والحالات من عصر Kerckhoffs إلى عصرنا هذا؛ أي بعد قرن ونيّف، تم تعديل تلك المبادئ لتلائم الأوضاع الحالية مع الحفاظ بجوهرها؛ لذا سنسرد هذه المبادئ كما أعلنها Kerckhoffs ثم سنشرحها بتفسير حديث.

المبدأ الأول: يجب أن يكون نظام التعمية غير قابل للكسر، إن لم يكن نظريًّا فعمليًّا على الأقل. كما نعلم أنه ليس ثمة نظام تعمية آمن بلا قيد إلا نظام (سِجلّ المرة الواحدة)، أو أي خطة تشابهه، وهو النظام الوحيد الذي بُرهِن على أنه غير قابل للكسر على المستويين النظري (الرياضي) والعملي، وفيما يتعلّق بهذه الأوقات، يمكن فهم المقصد الذي أراده Kerckhoffs من هذا المبدأ أن يكون نظام التعمية آمنًا حسابيًّا على الأقل، وصعب الكسر للوقت الآني، وهذا ما ينتهجه اليوم مصمّمو أنظمة التعمية وخوارزمياتها، وتتعلّق الصعوبة العملية لكسر خوارزميات التعمية بناحيتين: الأولى، التعقيد الحسابي بالنسبة إلى كسر خوارزميات التعمية المتماثلة. والثانية، المعضلة الرياضية بالنسبة إلى كسر خوارزميات التعمية غير المتماثلة.

المبدأ الثاني: يجب ألا يُحدِث اكتشاف تفاصيل عمل نظام التعمية أي مشكلة لدى مستخدميه. هذا المبدأ هو المبدأ الشهير في مجتمع التعمية، وهو الشرط الأساسي الذي يجب أن تحققه خوارزمية التعمية، وإنّه لواضح من نص المبدأ أن وقوع تفاصيل عمل نظام التعمية كاملةً بأيدي الخصم ينبغي ألا يخترق أمن المعلومات التي تم تعميتها به، وإضافة إلى ذلك، ينبغي ألا تصنع معرفة تطبيقه (source code) أيضًا أي مشكلة،

وينص هذا المبدأ في الوقت الحالي على أنه يجب أن تكمن سريّة نظام التعمية فقط في المفتاح الذي يستخدمه المشاركون في الاتصال، وليس في تفاصيل عمل النظام، ويجب إذًا على مصمّم خوارزمية التعمية أن يجعل جميع الأسرار الضرورية لأمان المعلومات التي ستعمَّى بها قدر الإمكان متمثّلة فقط في المفتاح الذي سيتم استخدامه، ثم يجب عليه بعدها أن ينشر الخوارزمية للعلن؛ كي يتم إخضاعها للبحث والدراسة، حتى من قِبَل الخصوم، من أجل استكشاف نقاط الضعف غير المُدركة وتحسينها. في الواقع، الوضع مختلف جدًّا بالنسبة إلى وكالة الأمن القومي الأمريكي NSA، إذ إنَّ الوكالة لم ولن ترغب أبدًا في نشر خوارزميات وأنظمة التعمية التي لديها للعلن، والسبب ليس لأنَّ السريّة التي تتبعها في ذلك قد حسّنت من أمن خوارزمياتها ونتائج عملها في التعمية، إنما لكي لا يستفيد أعداء الولايات المتحدة من خبرتها ومعرفة تفاصيل تلك الخوارزميات، وقد تكون الوكالة في هذا الأمر على صواب؛ لأنَّ مقراتها تضم أفضل وأذكى خبراء التعمية وتحليلها في العالم، وهؤلاء الخبراء هم الذين يتولون مهمة تصميم أنظمة التعمية، وهم الذين يحاولون كسرها من أجل اختبارها واكتشاف نقاط الضعف فيها.

المبدأ الثالث: ينبغي أن يكون المفتاح المستخدم في النظام سهل التذكّر، وقابلًا للتغيير في أي وقت. إنَّ سهولة حفظ المفتاح المستخدم أمر ضروري في جميع الأوقات، وينبغي أن يكون المفتاح، عندما يتم الاتفاق عليه بين طرفي الاتصال، سهل الحفظ دون تدوينه على أي وسيلة، ومن ثم سهل التذكّر في كل مرة يتم استعماله، وتحقق خوارزميات التعمية المتماثلة الحديثة هذا الأمر، إذ تمكّن المستخدم من أن يصنع مفتاحه الخاص من كلمة سر سهلة الحفظ والتذكّر، وأمّا بالنسبة إلى خوارزميات التعمية غير المتماثلة فيتولّى مهمة إنشاء المفتاح أحيانًا نظام التعمية نفسه، وقد يتطلّب تخزينه على وسيطٍ ما نظرًا لكبر حجمه، ولكن لا يعني ذلك أن يكون سهل التخمين، فيجب أن يحقق المفتاح العشوائية وسهولة الحفظ معًا، إضافة إلى ذلك، ينبغي لنظام التعمية أن

يكون ديناميكيًّا فيما يتعلّق بإمكانية تغيير المفتاح المستخدم إلى مفتاح جديد، وذلك عند رغبة المشاركين في الاتصال.

المبدأ الرابع: يجب أن تكون الرسائل المعمّاة سهلة النقل عبرَ التليغراف. لقد انخفض استخدام التليغراف في الوقت الحالي، فينبغي أن تكون الرسائل المعمّاة بالشكل الذي يسمح بنقلها عبرَ وسيلة الاتصال بسهولة ودون أخطاء[1]، وهذا يشير إلى أنه يجب على تلك الرسائل المعمّاة أن تضم محارف الأبجدية المعرّفة في وسيلة الاتصال فقط، ويتحقق هذا المبدأ حاليًّا من خلال استعمال نظام الترميز بالأساس 64، حيث تُرمَّز فيه الرسائل المعمّاة قبل نقلها إلى الأطراف الأخرى، ويَسهُل إرسال الرسائل المرمّزة واستقبالها بالنظام Base64 دون أخطاء، وذلك لقابلية تعريف محارفه في وسيلة الاتصال (البريد الإلكتروني).

المبدأ الخامس: ينبغي أن تكون خطة التعمية سهلة التداول والنقل، وينبغي ألا يتطلّب استعمالها جهدًا أكثر من شخص واحد فقط. لقد صاغَ Kerckhoffs هذه المبادئ لبناء خطط تعمية عسكرية، وإذا كانت خطة التعمية عبارة عن آلة، وليست خوارزمية أو طريقة رياضية، فينبغي أن تكون سهلة الحمل والنقل، وفيما يخص العمل الميداني في أثناء الحرب، يتطلّب هذا المبدأ أن تكون خطة التعمية قابلة لتداولها بين المعنيين (ضباط الجيش) سواء كانت آلة أم طريقة رياضية، وأمّا للوقت الحالي فخطة التعمية متمثّلة في الطريقة الرياضية فقط. وهذه الطريقة هي مجموعة من الخطوات المرتّبة ترتيبًا ثابتًا وواضحًا، وإنَّ هذا التمثيل يجعلها سهلة التداول والنقل والنشر، وأيضًا ينبغي ألا يتطلّب استعمال خطة التعمية جهدًا أكثر من شخص واحد، فإذا كانت الخطة آلة تعمية، فمن الضروري ألا تحتاج إلى أكثر من شخص لإنجاز تعمية رسالة ما (وهذا شيء مهم لاعتبارات عدة، منها عدم توافر أكثر من شخص في مكان العمل

(1) قد ينجم الخطأ عن مشكلة في مسار شبكة الاتصال أحيانًا، وهذا الأمر لا علاقة له بالمبدأ.

خاصةً إذا كان هذا المكان حربيًّا)، وإن كانت الخطة رياضية فمن الضروري أيضًا أن تكون سهلة الاستعمال من قِبَل شخص واحد، وتجدر الإشارة إلى أن خوارزميات التعمية المتماثلة الحديثة صعبة التطبيق يدويًّا، ولهذا فإن البرمجيات الحاسوبية تجعل تنفيذها أسهل.

المبدأ السادس: ينبغي أن يكون نظام التعمية سهل الاستخدام، بحيث لا يتطلّب معرفة بإجراءات وقواعد كثيرة، ولا جهدًا ذهنيًّا. من الواضح أن هذا المبدأ يرتبط بالمبدأ السابق، إذ إنه من سهولة نظام التعمية سيُتاح استعماله من قِبَل شخص واحد، وعلى الرغم من أن المبدأ الأول ينص ضمنيًّا على أن تكون خطة التعمية متينة وصعبة الكسر ومعقّدة، إلا أنها ينبغي أن تكون سهلة الاستخدام في الوقت نفسه، وهذا ما ينص عليه المبدأ الحالي، وليسَ على مستخدم النظام، في أثناء تعمية أو فك تعمية رسالة، أن يبذل جهدًا ذهنيًّا كبيرًا لإنجاز المهمة، وأيضًا ليسَ عليه أن يكون ملمًّا بقواعد وإجراءات من أجل إتمام عملية التعمية أو فك التعمية، ونفترض دائمًا أن مستخدم النظام لا يفقه شيئًا بتفاصيله الرياضية الداخلية، ومن ثم فعليه فقط أن يقوم بإدخال المفتاح والنص الواضح أو النص المعمّى وإنجاز بعض الخطوات البسيطة، وثمة طرق تقليدية تتطلّب من مستخدميها أن يمتلكوا بعض الخلفيات الرياضية، مثل معمّي Hill ومعمّي Playfair، وأمّا في خوارزميات التعمية المتماثلة الحديثة فلا يمكن أبدًا تطبيقها يدويًّا حتى ولو توافرت لمستخدميها خلفيات متعددة عنها، وذلك بسبب تعدد خطواتها المعقّدة، وتتطلّب هذه الخوارزميات الحديثة بالتأكيد برمجيات حاسوبية لتطبيقها (باستثناء بعض أنظمة التعمية غير المتماثلة التي يمكن تطبيقها يدويًّا دون استعمال البرمجيات)، حيث لا تأخذ من المستخدم وقتًا أكثر من إدخاله النص الواضح أو النص المعمّى والمفتاح.

إذًا، أهم مبدأ من تلك المبادئ الستة السابقة هو المبدأ الثاني الذي يوصي بأن تكون تفاصيل عمل خطة التعمية معروفة للجميع، وألا تكون تلك المعرفة مصدر تهديد لأمن المعلومات المعمّاة بها، وأن تكمن سريّة النظام بأكمله في المفتاح المستخدَم،

وثمة مبدأ شهير في مجتمع التعمية وأمن المعلومات يخالف مبدأ Kerckhoffs الثاني، وهو مبدأ **الأمن عبر التعتيم** Security Through Obscurity.

ينص مبدأ الأمن عبر التعتيم على استعمال سريّة تفاصيل عمل نظام التعمية، إضافة إلى سريّة التطبيق، لتحقيق أمن المعلومات، ومن المحتمل جدًّا أن تكون أنظمة التعمية التي تعتمد على مبدأ الأمن عبر التعتيم حساسة تجاه الهجمات الكامنة، وقد تمتلك نقاط ضعف كثيرة، وعلى الرغم من ذلك، يعتقد مصمّمو تلك الأنظمة أنها آمنة، وإن كان ثمة عيوب بها فهي غير ظاهرة وغير معروفة، ومن غير المحتمل أن يكتشفها الخصوم ومحللو التعمية، والخوارزميات المقيّدة هي خيرُ مثال على مبدأ الأمن عبر التعتيم.

لنكن أكثر وضوحًا بشأن سريّة المفتاح المستخدَم، ونصَّ الافتراض الأساسي في التعمية على أن يكون فضاء المفتاح K معروفًا، فهذا يعني أن جميع عناصره معروفة بدلالة حجمه وأبجدية التعريف المستخدمة، لكن الموضوع هنا يكمن في أن تتمثل سريّة المفتاح في العجز الذي يواجهه الخصم في العثور عليه من بين مجموعة كبيرة من المفاتيح. إذًا المفتاح موجود، وهو عنصر من أحد عناصر فضاء المفتاح المرافق لنظام التعمية؛ لذا فمن أجل تعقيد المهمة أمام الخصم، يقوم مصمّمو الخوارزميات بجعل فضاء المفتاح ضخمًا قدر الإمكان دون التساهل في قوة الخوارزمية نفسها.

يُعمِّم Bruce Schneier مبدأ Kerckhoffs الثاني ليشمل جميع أنظمة الأمن الأخرى، وإنَّ كل سر يبقى سرًّا في نظام أمني ما لديه بالتأكيد نقطة ضعف محتملة قابلة للهجوم، وينبغي أن تكون الأسرار المطلوب الاحتفاظ بها في النظام الأمني، هذا إن اقتضى الاحتفاظ بها، من المستويات التي إذا تم اختراقها (ولو بالمصادفة) لا تسبب خسائر كبيرة، وهذا الأمر مشابه جدًّا لنظام تعمية قوي، إذ يسعى مصمم الخوارزمية إلى أن يجعل جميع الأسرار المرتبطة بالنظام كامنة بشكل كلي تقريبًا في المفتاح السري

المستخدم، وإذا تم اكتشاف المفتاح فينبغي أن يكون ثمة بديل لإصلاح هذا الخرق؛ البديل هو توليد مفتاح جديد واستعماله، وأمّا الخسارة الكبيرة في نظام التعمية المقيّد فهي اختراق المعلومات المعمّاة به بعد التعرّف إلى تفاصيله، وهذا ما سيحدث إذا تم اعتبار النظام نفسه سرًّا. وكقاعدة عامة «كلما امتلك النظام الأمني أسرارًا أكثر في مضامينه، كان ضعيفًا وعُرضة للهجوم، وكلما كانت أسراره أقل، كان أكثر قوة».

6.6 مبادئ استخراج المعمى و(الهجمات) على إجراءات التعمية أو خدماتها

لقد عرّفنا استخراج المعمى أو تحليل التعمية مسبقًا، (**أو كسر الشفرة**) cryptanalysis or code breaking على أنّه فك تعمية المعلومات السريّة المحمية دونَ معرفة المفتاح المستعمل، وتُدعى المحاولة المقصودة في نطاق تحليل التعمية الهجوم التعموي، وبالتعريف، فـ**الهجوم التعموي** Cryptographic Attack **هو المحاولة المتعمَّدة لتعطيل خدمة ما أو أكثر من خدمات التعمية أو إفساد بروتوكول تعمية أو اختراق أمن خوارزمية تعمية.**

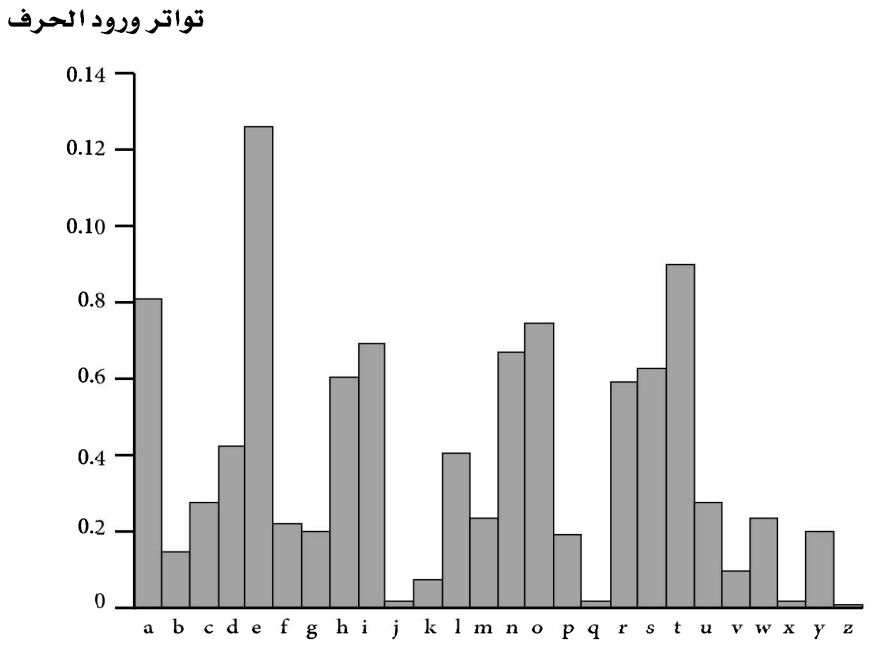
علم استخراج المعمى أكثر تعقيدًا من علم التعمية، ويحتاج إلى معارف في الرياضيات واللسانيات (وفي أيامنا إلى أدوات معلوماتية جبارة).

وأثبتت البحوث أخيرًا أن يعقوب الكندي، فيلسوف العرب (801–873 م) هو مؤسس هذا العلم،

وواضع أول كتاب فيه بعنوان (رسالة في استخراج المعمى) وهي رسالة مذهلة في معلوماتها[1].

(1) (التعمية واستخراج المعمى عند العرب) الجزء الأول والجزء الثاني، تأليف الدكاترة: محمد مراياتي، ويحيى مير علم، وحسان الطيان.

تواتر ورود حروف اللغة الإنجليزية



ويذكر الكندي أن طرق استخراج المعمى تعتمد على ثلاثة مبادئ: **الأول** هو إحصاء تواتر الحروف، أو الأشكال، أو الرموز في النص المعمى بالإعاضة، ومقارنته مع إحصاء تواتر الحروف في اللغة التي كتب بها النص المعمى كالعربية مثلًا، ويقدم الكندي إحصاءه لتواتر الحروف في اللغة العربية، ويذكر أن هذا المبدأ لا ينطبق إلا عندما يكون النص طويلًا إلى حد يسمح فيه عدد الحروف بانطباق القانون الإحصائي عليه (قانون الأعداد الكبيرة في الإحصاء!).

أما المبدأ **الثاني** فهو الاستفادة من تقارن الحروف وتنافرها في اللغة، فهناك حروف تتوالى كثيرًا مثل الألف واللام في (ال) التعريف، حيث تواترها عالٍ جدًّا؛ لذلك يجب البحث عن هذا التقارن في النص والاستفادة منه في استخراج المعمى، وهناك حروف لا تقترن تقديمًا، وأخرى تقترن تأخيرًا؛ أي لا تأتي قبل بعضها أو بعد بعضها،

ويعطي الكندي في رسالته دراسة وافية ومدهشة عن اقتران الحروف وتنافرها، وعن الكلمات الثنائية والثلاثية الأكثر تواترًا في اللغة العربية، مثل (من، عن، أن، في..) و(إلى، على، بلا،...).

أما المبدأ **الثالث** فهو (الكلمة المحتملة) probable word؛ أي ما يُستعمَل في الرسائل أو النصوص من عبارات الاستهلال والألقاب وما إليها، وهذه المبادئ الثلاثة لا تزال صحيحة ومستعملة في استخراج المعمى حتى يومنا هذا، ويُعدّ الكندي مخترع هذا العلم وواضع مبادئه.

وكما سبق هناك طرق غير قابلة للاستخراج، مثل طريقة (سِجلّ المرة الواحدة) وهي الطريقة الوحيدة التي تمَّ البرهان على أنها لا تُستخرج، أما طرق التعمية الأخرى فيمكن استخراجها نظريًّا، ويعتمد ذلك على الوسائل والوقت المتاح للمستخرج. على أن بعض الطرق تحتاج إلى وقت ووسائل غير متوافرة؛ لذلك تُعدّ غير قابلة للاستخراج عمليًّا.

والخلاصة هي أن ثمة أربعةِ مبادئ أساسية في استخراجِ المُعَمَّى أو حلِّ التعميةِ، درجَ العربُ على استخدامِها،

وبرعوا فيها منذ مدة مبكرةٍ على نحوٍ مدهشٍ، وهذه الطرقُ هي:

1. استعمالُ عددِ الحروفِ المستخدمةِ لتحديدِ اللغةِ المُعَمَّاة.
2. استعمالُ تواترِ ورودِ الحروفِ في النصِّ.
3. استعمالُ تواترِ ورودِ ثنائياتِ الحروفِ وثلاثياتها وغيرِها، أو ما سمَّوه ائتلاف الحروفِ وتنافرها.
4. استعمالُ الفواتح التقليديةِ المُحْتَمَلَةِ للرسائلِ، وهو ما سُمِّي حديثًا الكلمة المُحْتَمَلَة الورودِ.

يشتمل الملحق رقم (2) على ثلاثة أمثلة تراثية في استخراج المعمى.

من طرق استخراج التعمية التي تستعمل المفتاح المتناظر:

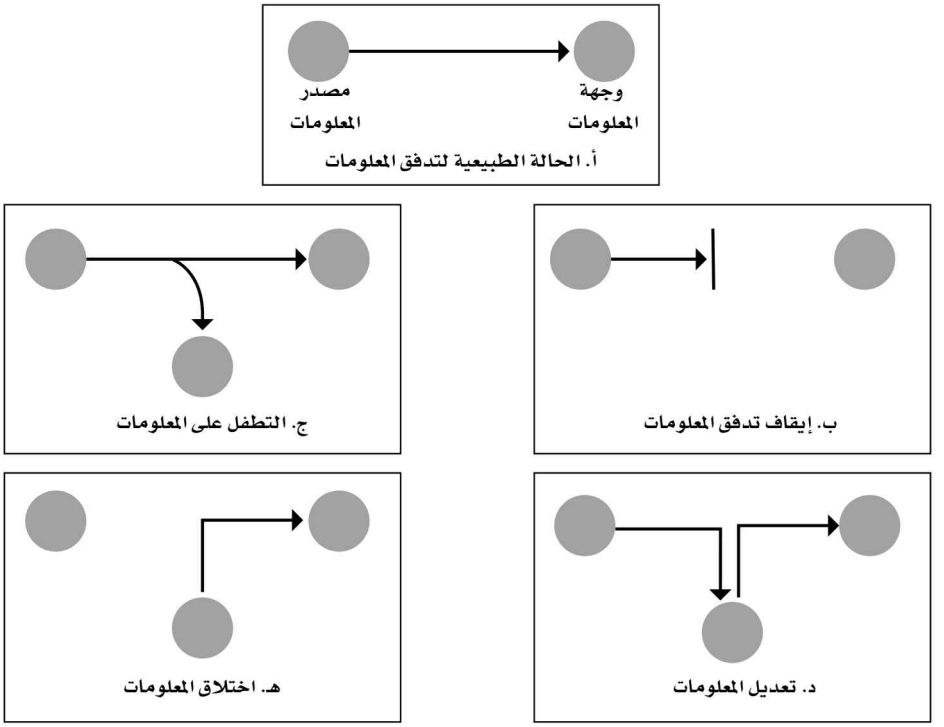
- التحليل (الأعمى) أو تجربة كل المفاتيح باستعمال حواسيب عملاقة.
- التحليل التفاضلي، وقد استخدم في استخراج تعمية المعيار الأمريكيDES ذي المفتاح القصير.
- التحليل الخطي.

وسنتطرق فيما يأتي إلى أهم (الهجمات) المنشورة في استخراج المعمى والهجمات على خدمات التعمية بشكل عام ضمن إطار أمن المعلومات، وإنَّ تصنيف هجمات التعمية متعدد ومتنوع، حيث إنَّ كل مرجع يعتمد على نموذج ما، وسوف نسرد في الفقرة الآتية هجمات التعمية وفق ثلاثة نماذج رئيسة: الهجوم على **خدمات التعمية**، والهجوم على **بروتوكولات التعمية**، والهجوم على **خوارزميات التعمية**.

1.6.6 الهجوم على خدمات التعمية

يتمثّل الهجوم على خدمة ما من خدمات التعمية في تعطيل أداء هذه الخدمة وعملها، ويتمثل نجاح الهجوم في عدم استطاعة المستخدم الشرعي تلقّي هذه الخدمة، ويُصوِّر Stallings في مرجعه مبدأ هذه الهجمات انطلاقًا من أنَّ الحالة الطبيعية لأداء الخدمة وإتمامها تتمثّل في تدفّق المعلومات بشكل سليم ومباشر من مصدرٍ ما إلى وجهةٍ ما؛ أي عندما تصل المعلومات سليمة إلى المكان المقصود تكون الخدمة قد أُدّيت. يعرِّف الشكل (1-4 أ) الحالة الطبيعية لتدفّق المعلومات Normal flow دون أي هجوم.

الشكل (4_1) الهجمات المحتملة على خدمات التعمية.



- **إيقاف تدفّق المعلومات** Interruption. عندما تتدفّق المعلومات عبر الشبكة من مصدرٍ ما إلى وجهةٍ ما يقوم المهاجم باعتراضها ومنع إيصالها إلى تلك الجهة المطلوبة، ويُعَدّ هذا الهجوم هجومًا على خدمة **توافر المعلومات** Availability[1]. يوضّح الشكل (4–1 ب) هذا الهجوم.
- **التطفّل على المعلومات** Interception. عندما تتدفّق المعلومات المحمية من مصدرٍ ما إلى وجهةٍ ما يقوم المهاجم بالتجسس عليها، والحصول على نسخة صافية واضحة منها، ويُعدّ هذا الهجوم هجومًا على خدمة **السريّة** confidentiality. يعطي الشكل (4–1 ج) صورة عن هذا الهجوم.

(1) في الحقيقة، إنَّ خدمة توافر المعلومات ليست من خدمات التعمية، ولكن الهجوم عليها يُعدّ جزءًا من الهجمات الموجَّهة على خدمات التعمية.

- **تعديل المعلومات** Modification. عند تدفّق المعلومات وفق المسار الطبيعي لها يعترضها المهاجم ليقوم بتعديلها، إمّا بإضافة بيانات أخرى عليها، أو إزالة بيانات منها، أو استبدال بيانات، ثم يرسلها بعد ذلك إلى وجهتها الطبيعية المفترَضة، ويُعدّ هذا الهجوم هجومًا على خدمة **سلامة البيانات** Data integrity. انظر الشكل (1–4 د).
- **اختلاق المعلومات** Fabrication. ليس ثمة تدفق لمعلومات حقيقية إلى وجهة طبيعية شرعية، فيقوم المهاجم في هذه الحالة باختلاق بيانات وتركيبها وإرسالها إلى وجهة ما على أنها معلومات قادمة من مصدر شرعي حقيقي، ويُعدّ هذا الهجوم هجومًا على خدمة **استيقان منشأ البيانات** Authentication. انظر الشكل (1–4 هـ).

2.6.6 الهجوم على بروتوكولات التعمية

قبل الحديث عن الهجمات المحتملة على بروتوكولات التعمية، دعنا نعرّف أولًا البروتوكول التعموي باختصار. يُعرَّف **البروتوكول التعموي** Cryptographic Protocol كما جاء في بأنه سلسلة من الخطوات المرتّبة ترتيبًا واضحًا، حيث يستعمل تقنية التعمية وتقنيات أخرى مرتبطة بها من أجل إنجاز مهمة ما، مثل إيصال المعلومات السريّة إلى أصحابها الحقيقيين والكشف عن الخصوم الواقعين في وسط قنوات الاتصال، ويقوم بتلك الخطوات طرفان أو أكثر من الأطراف الشرعية المشاركة، وقد تكون بعض الأطراف غير شرعية؛ لذا يهتم البروتوكول التعموي بالكشف عنها وفضحها.

ويتمثل الهجوم على بروتوكول التعمية في إحباط وإفشال خطوة ما أو أكثر من خطواته، ويتمثل أيضًا في المشاركة في هذا البروتوكول بوصفه طرفًا شرعيًّا دون علم بقية الأطراف، وإنَّ بروتوكولات التعمية كثيرة ومتنوعة، والهجمات عليها متنوعة، ولها

أشكال عدة، وثمّة نوعان عامان من الهجمات المعروفة على بروتوكولات التعمية هما: الهجوم السلبي، والهجوم الفعّال.

1.2.6.6 الهجوم السلبي Passive Attack

يُسمى أيضًا **الهجوم غير الفعّال**. يقوم الخصم أو المهاجم في هذا النوع بمراقبة قناة الاتصال التي يجري فيها تنفيذ البروتوكول بين الأطراف الشرعية المشاركة، والفائدة التي يجنيها هي الحصول على المعلومات المتبادلة وقراءة الرسائل دون أن يُكتشَف (أو على نحوٍ أدق دون أن يُكتشَف وجوده)، فإنَّ الخصم في هذه الحالة لا يأتي بأي حركة تفسد إتمام البروتوكول، وهو بذلك يُعدّ طرفًا غير محسوس به في هذا البروتوكول، ومن صفات هذا الهجوم أنه صعب الكشف، ولهذا عادةً ما تسعى بروتوكولات التعمية إلى أن تمنعه بدلًا من أن تكتشفه؛ لذا من الضروري جدًّا على بروتوكول التعمية أن يتوقّع جميع الاحتمالات التي قد يصادفها، خاصةً إذا كانت حالات اختراق أو تلاعب، وثمّة نوعان من الهجمات السلبية: التجسس، وتحليل الحركة.

التجسّس Tapping.

إنَّ هذا الهجوم هو أبسط هجوم معروف، وليس في هذا الهجوم أي معلومات محمية أو معمّاة (على الرغم من أنها قد تكون سريّة)، إذ تمر المعلومات والرسائل بشكلها الطبيعي عبر قناة اتصال عادية (من المفترض أنها غير آمنة)، ويتجسّس المهاجم ببساطة على قناة الاتصال للاطلاع على المعلومات المتبادلة بين طرفين شرعيين، ومن أمثلة هذا الهجوم: التجسّس على محادثة هاتفية، أو الاطلاع على رسالة بريد إلكتروني عادية غير معمّاة، ويُمكن صد هذا الهجوم بسهولة من خلال استعمال تقنية التعمية، سواء لحماية المحادثات الهاتفية أو لحماية التبادلات الإلكترونية، ويُسمَّى هذا الهجوم أيضًا **تحرير محتوى الرسالة** Release of message contents.

تحليل الحركة Traffic Analysis.

يفترض هذا الهجوم تعمية المعلومات والرسائل التي تمر عبر قنوات الاتصال غير الآمنة، ويراقب المهاجم في هذا النوع حركة الاتصالات والرسائل المعمّاة الجارية بين الأطراف الشرعية، ويقتصر عمل المهاجم من خلال مراقبته لحركة الاتصالات المعمّاة على محاولة معرفة المكان الذي تصدر منه الرسائل، والمكان الذي ستتوجه إليه، وطول تلك الرسائل، وزمن إرسالها، والاستفادة من النماذج التكرارية لنصوص بعضها، إضافة إلى معرفة تطابقها مع الأحداث الخارجية للمتصلين، مثل عقد اجتماع في زمنٍ ما، وينبغي أن تُساعد جميع المعلومات السابقة المهاجم على تخمين طبيعة الاتصالات على الأقل، والأفضل أن تُساعده على اكتشاف مضمون بعضها. وكقاعدة، كلما كان عدد الرسائل التي يتم رصدها واختبارها أكبر، زادَ احتمال نجاح هذا الهجوم، ويتطلّب هذا الهجوم جهدًا ووقتًا كبيريَن نسبيًّا لكي ينجح، وهو في بعض الأحيان صعب التطبيق بالنسبة إلى الأفراد العاديين، وتستخدم استخبارات بعض الدول هذا النوع من الهجوم للتجسّس على اتصالات الدبلوماسيين الأجانب المقيمين على أرضها.

2.2.6.6 الهجوم الفعّال Active Attack

يتميّز الهجوم الفعّال بالنشاط حيال الأذى الذي يسببه في أثناء تنفيذ بروتوكول ما أو حتى في وقت لا يتم من خلاله تنفيذ أي بروتوكول، ويحاول الخصم في الهجوم الفعّال التأثير في مجريات الاتصال القائم بين طرفين شرعييَن عبر خط قناة غير آمنة، وتتضمن الحركات التي قد يقوم بها الخصم في الهجوم الفعّال: -1 تعديل رسالة ما من خلال استبدال بياناتها أو حذف أجزاء منها أو إضافة بيانات إليها. -2 إنشاء رسائل ومعلومات جديدة ومزيّفة وإرسالها إلى طرفٍ ما على أنها قادمة من طرف شرعي. -3 خداع أحد طرفي الاتصال (أو كليهما) وإيهامه بأنه طرف شرعي. -4 إعاقة

تنفيذ الاتصال أو حتى تخريب القناة بأكملها. -5 قد يستطيع المهاجم أحيانًا الوصول إلى حاسب المستخدم وتخريب بياناته (يتم هذا عن طريق إصابة الحاسب بفيروس).

إذًا، تتطلّب الهجمات الفعّالة من الخصم التأثير في خطوة واحدة أو أكثر من خطوات البروتوكول، وفي أحيان أخرى التأثير في أحد طرفي الاتصال أو كليهما، والتلاعب بهما دون تنفيذ أي بروتوكول[1]، ولذلك تُعدّ الهجمات الفعّالة أكثر خطورة من الهجمات السلبية بسبب تأثيرها التخريبي، وليس بالضرورة أن يكون المهاجم طرفًا خارجيًّا غير شرعي، فقد يكون أحد الأطراف الشرعية المشاركة، وقد يكون مدير النظام، وفي هذه الحالة يُسمّى المهاجم **الغشّاش** Cheater، ومن المحتمل أيضًا أن يُوجَد أكثر من مهاجم ينفّذون مهمة واحدة، وخلافًا لنمط الهجوم السلبي يمكن اكتشاف وقوع الهجوم الفعّال بسهولة (وهذا بسبب نشاطه التفاعلي المحسوس)؛ ولذلك تسعى تقنيات التعمية إلى اكتشاف هذا الهجوم ومنع وقوعه، **وثمّة ثلاثة أنواع من الهجمات الفعّالة** هي: هجوم انتحال الشخصية، وهجوم الشخص الذي في الوسط، وهجوم إعادة التشغيل.

أ. هجوم انتحال الشخصية Attack Impersonation.

يُسمّى أيضًا **التنكّر** Masquarade، وينتحل الخصم في هذا الهجوم هوية أحد الأطراف الشرعية المشاركة في الاتصال، ثم يراسل الأطراف الأخرى على أنه ذلك الطرف الذي انتحل اسمه بوصفه مشاركًا حقيقيًّا في الاتصال، ويحدث هجوم انتحال الشخصية في عالم الواقع كثيرًا، والدليل على ذلك هو تلك المحاولات التي يخدع فيها الخصم الأطراف عبر الاتصال بهم هاتفيًّا والتحدّث معهم على أنه أحد الأقارب أو الأصدقاء بهدف سلب بعض المعلومات والإيقاع بهم، وينجح الهجوم في هذا الشكل من خلال استعمال تقنيات تقليد الأصوات بعد تسجيلها، وأمّا الحالات الأكثر واقعية فتكمن في غرف الدردشة على الإنترنت، وثمّة كثير من الناس الذين يقعون ضحايا عمليات

(1) ما يقصد هنا هو البروتوكول التعموي فقط.

احتيال وخدع ينفّذها خصوم بإحكام ضدهم، وتتمثّل هذه الخدع أحيانًا في تنكّر الفتاة بهوية شاب والتحدّث مع شاب آخر على هذا الأساس أو العكس، وأحيانًا تكون نتيجة هذا الاحتيال أكثر خطورة من مجرّد ضحايا حديث الحب والغرام وسلب المعلومات، فقد يكون هذا الهجوم انتحال شخصية بهدف تنفيذ عملية منظمة والإيقاع بأطراف بريئة، ومع الأسف تحدث هذه الحالات كثيرًا في عالم الواقع.

يمكن صَدّ هذا الهجوم في حالات معينة من خلال استخدام أحد تمثيلات[1] بروتوكول **التحدّي والرد** Challenge and Response Protocol، فمثلًا لو كان الطرفان المشاركان في الاتصال يعرفان بعضهما مسبقًا (أقارب أو أصدقاء مثلًا)، بإمكانهما الاستيقان من بعضهما عن طريق تنفيذ هذا البروتوكول، ويُسمّى الاستيقان في هذه الحالة استيقان الطرف أو إثبات الهوية (انظر 1-4)، ولنفترض في هذا التمثيل من بروتوكول التحدّي والرد أنَّ بوب يرغب في مراسلة أليس، فلكي يستيقن كلٌّ من أليس وبوب من هوية بعضهما يحتاجان إلى تنفيذ خطوات البروتوكول على النحو الآتي:

1. ترسل أليس رسالة إلى بوب تحتوي على كلمة ما طالبةً منه تعميتها بالمفتاح السرّي الذي تشاركه به.
2. يقوم بوب بتعمية الكلمة وإرسال الناتج برسالة إلى أليس مُرفقة بكلمة أخرى جديدة طالبًا منها تعميتها بالمفتاح السرّي نفسه.
3. تتحقق أليس من صحة الناتج، وتتأكد من أنه بوب نفسه، ثم تُعمّي الكلمة التي أرسلها بوب، وبعدها ترسل الناتج إليه.
4. يتحقق بوب من الناتج، ويتأكّد بذلك من أنها أليس نفسها.

---

(1) ثمّة أكثر من تمثيل لبروتوكول التحدّي والرد، انظر الفصل الثاني من:
Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2001.

ثمّة حالة يَفشل فيها هذا الشكل من البروتوكول تمامًا، فلو استطاع خصمٌ ما الحصول على المفتاح السرّي من بوب بطريقة أو بأخرى، وهو المفتاح المشترك مع أليس، لتَمَكّن من تنفيذ بروتوكول التحدّي والرد بنجاح والحديث مع أليس على أنه بوب، وبالإمكان تنفيذ بروتوكول التحدّي والرد على هذا النحو في غرف الدردشة وفي رسائل البريد الإلكتروني.

ب. هجوم الشخص الذي في الوسط Man-In-The-Middle Attack.

ويُعرَف اختصارًا بـ MITM. يقع هذا الهجوم عندما يتصل الطرفان الشرعيان عبر قناة غير آمنة في ظل استعمال تقنية التعمية بالمفتاح العام، ويتركّز الخصم في هذا الهجوم في وسط قناة الاتصال محاولًا قراءة الرسائل السريّة المتبادلة وتعديلها (إن رغبَ في ذلك) دون علم الطرفين الشرعيين المشاركين. معياريًّا، يُعدّ هجوم الشخص الذي في الوسط ناجحًا في بروتوكولات تبادل المفاتيح العامة التي لا تستعمل أي طريقة للاستيقان.

ولإيضاح فكرة هذا الهجوم جيدًا، سوف نستعرض بروتوكول تبادل المفاتيح العامة الأساسي مع محاولة الخصم خداع أليس وبوب. يرغب أليس وبوب في تبادل الرسائل السريّة من خلال استعمال كُلٍّ منهما المفتاح العام للآخر.

1. ترسل أليس إلى بوب مفتاحها العام. يعترض الخصم الرسالة، ويستبدل ذلك المفتاح بالمفتاح العام الخاص به، ثم يرسله إلى بوب، ويحتفظ بالمفتاح العام لأليس.
2. يرسل بوب إلى أليس مفتاحه العام. يعترض الخصم الرسالة، ويستبدل ذلك المفتاح بمفتاح عام آخر خاص به، ثم يرسله إلى أليس، ويحتفظ بمفتاح بوب العام.

3. عندما ترسل أليس رسالة إلى بوب، تُعمّيها بمفتاحه العام. ولأن المفتاح العام الذي استعملته أليس عائدٌ للخصم، يعترض هذا الأخير الرسالة، ويفك تعميتها باستخدام مفتاحه الخاص، ثم يقرؤها، ويعدّل عليها إن تطلّب الأمر، وبعد ذلك يُعمّيها باستعمال المفتاح العام لبوب، ويرسلها إليه.
4. يستقبل بوب الرسالة في ظرف مدة زمنية عادية ومقبولة (أي لا يوجد فيها أي تأخير).
5. يكرّر الخصم الخطوة (3) مع بوب.

لن يلحظ أيٌّ من بوب وأليس أن ثمّة طرفًا ثالثًا غير شرعي يتجسس على رسائلهما، ويقرؤها دون رقيب. يعلم كلٌّ من بوب وأليس أنهما يتحدّثان عبر قناة غير آمنة، ويستخدمان التعمية من أجل تأمين اتصالاتهما، ولكنهما لا يدركان وجود شخص ثالث يطّلع على أسرارهما.

ومن أجل جعل الاتصال آمنًا، يجب أن يضمن كلا الطرفين سلامة المفاتيح العامة التي يتبادلانها، ولكن لا يعني ذلك أن عليهما تبادلها بطريقة سريّة أو عبر قناة آمنة، فالبروتوكول الذي يقترح هذا الحل يُعدّ فاشلًا بكل المقاييس، والمفاتيح العامة، كما هو واضحٌ من اسمها، ينبغي أن تكون على مرأى من الجميع ودون تحفّظ.

يمكن إحباط هجوم الشخص الذي في الوسط من خلال تنفيذ بروتوكول **الضم** Interlock Protocol. اقترح Rivest وShamir بروتوكول الضم من أجل اكتشاف وجود الخصم الواقع في وسط قناة الاتصال، ولا يمنع هذا البروتوكول الخصم من محاولته تلك، ولكنّه يُنذر الطرفين من أول مرة بوجوده. (انظر أيضًا المرجع).

ثمّة فرق بين هجوم الشخص الذي في الوسط وانتحال الشخصية المذكور سابقًا، ويمكن التمييز بين هاتين الهجمتين من خلال النظر إلى عدد المشاركين في الاتصال، وإنَّ عدد المشاركين في هجوم الشخص الذي في الوسط هو ثلاثة (أليس - بوب -

الخصم)، وأمّا في هجوم انتحال الشخصية فعدد المشاركين هو اثنان فقط (المرسل / المستقبل / الخصم)؛ لأنَّ الخصم ينتحل هوية إمّا المرسل أو المستقبل.

ج. هجوم إعادة التشغيل Replay Attack.

يسجّل الخصم في هذا الهجوم رسائل قديمة من بروتوكول ما عن طريق حفظ خطوات عدة منه، ثم إعادة استعمالها لاحقًا من أجل إعادة تنفيذ تلك الخطوات مع أحد الطرفين الشرعيَين اللذين قاما بتنفيذ البروتوكول نفسه سابقًا، ويسجّل الخصم في هذا الهجوم الخطوات، ويحتفظ بالمعلومات والمراسلات المطلوبة في أثناء تنفيذ البروتوكول بين الطرفين الشرعيَين دون علمهما، ويتضح من ذلك أن للمهاجم مهمتين: الأولى تتم ضمن إطار هجوم كامن، وهي المهمة التي يسجّل فيها المعلومات والمراسلات، والثانية تتم ضمن إطار هجوم فعّال يخدع فيها أحد الطرفين.

يمكننا أن نعدّ هجوم إعادة التشغيل جزءًا من هجوم انتحال الشخصية؛ وذلك لأن عدد المشاركين في كلتا الهجمتين نفسه، ولكن في هجوم إعادة التشغيل سيبدأ الخصم بالتنفيذ، ومن ثم سيكون هو المرسل، وعلى نحوٍ أدق، يمكننا اعتبار هجوم إعادة التشغيل حالة أو مثالًا عن هجوم انتحال الشخصية، ونستطيع صد هجوم إعادة التشغيل من خلال استعمال **الأختام الزمنية** Timestamps.

د. هجوم الحرمان من الخدمة Denial-of-Service Attack.

ثمة هجوم يرتبط ببروتوكول اتصال، ولكن ليس له علاقة بالتعمية، وهو هجوم الحرمان من الخدمة، ويُشَنّ من وسط قناة الاتصال على شبكة حاسوبية، فيؤدي إلى تحميلها بما يفوق طاقتها، ومن ثم إلى نقص الموارد المتاحة، ومن ثم منع المستخدم الشرعي من الاستفادة من تلك الموارد، ومن الأمثلة الواقعية على هذا الهجوم: منع الخصم وصول الرسائل إلى الطرف المعني بها، أو قيامه بتعطيل الشبكة بأكملها من خلال تحميلها رسائل تفوق طاقتها من أجل الحط من مستوى أدائها.

ثمة أشكال أخرى من الهجمات على بروتوكولات التعمية، ومن الممكن أن تظهر هجمات جديدة، ولكن كيف نعرف أن الهجوم هو هجوم على بروتوكول تعموي! عندما يقوم الهجوم على قناة الاتصال، ويُوجَّه على أحد تقنيات التعمية أو خدماتها فهو افتراضيًّا هجوم على بروتوكول تعموي، والتنفيذ لا يتم إلا في وسط قناة الاتصال سواء أكان سلبيًّا أم فعالًا.

3.6.6 الهجوم على خوارزميات التعمية

يُطبَّق هذا الهجوم على خوارزميات التعمية وخططها. إنَّ هذا النوع ليس بإستراتيجية لإحباط بروتوكول أو إفساد خدمة ما، وإنما طريقة عملية من أجل الوصول إلى الهدف النهائي، وهو الحصول على النص الواضح، ويتمثّل الهدف النهائي في الهجوم على خوارزميات التعمية في استعادة النص الواضح لنص معمّى مطلوب، وأما الهدف الوسيط فيتمثّل في الحصول على المفتاح المستعمل (أو استنتاجه) من أجل استعادة أي نص واضح مستقبلي، وقد يتمثّل الهدف الوسيط أيضًا في استنتاج (أو ابتكار) خوارزمية بديلة تسمح بالوصول إلى الهدف النهائي، وكما هو جلي، فإن الهدف الوسيط يُعدّ أهم من الهدف النهائي؛ كونه سيصبح وسيلة دائمة ومتوافرة للوصول إلى الهدف النهائي بسهولة، ويَفترض الهجوم على خوارزميات التعمية أنَّ المهاجم على معرفة تامة بالخوارزمية المستعملة.

ثمة **ستة أنماط رئيسة** من الهجمات الموجَّهة على خوارزميات التعمية هي: هجوم النص المعمَّى فقط، وهجوم النص الواضح المعلوم، وهجوم النص الواضح المختار، وهجوم النص الواضح المختار المتكيِّف، وهجوم النص المعمّى المختار، وهجوم النص المعمّى المختار المتكيِّف، وسوف نتحدث هنا عن النمط الأول فقط بوصفه مثالًا على هذا النوع من الهجوم على خوارزمية التعمية، وفي حال الرغبة في الاطلاع على الأنماط

الخمسة الأخرى، فيمكن العودة إلى المرجع: (المدخل إلى علم التعمية، تأليف: ساري خالد 2015م)[1]، ولكن تذكّر أن المهاجم في كل نوع لديه اطلاع تام على خطة التعمية[2].

هجوم النص المعمّى فقط Ciphertext–only Attack.

يمتلك المهاجم في هذا النمط النص المعمّى فقط c (أو مجموعة من النصوص المعمّاة c_1، c_2،....، c_i) المقابل لنص واضح m تم تعميته بمفتاح e:

$$c = E_e(m)$$

حيث $m \in M$ ، $c \in C$، $e,d \in K$.

يقتصر عمل المهاجم (محلل التعمية) على دراسة خصائص النص المعمّى c إمّا من أجل استعادة النص الواضح المقابل m بوصفه هدفًا نهائيًّا، أو لاستنتاج المفتاح d لفك تعمية نصوص مستقبلية معمّاة بالمفتاح e.

يمكن نمذجة هجوم النص المعمّى فقط على النحو الآتي (انظر المرجع):

إذا توافر للمهاجم $c_1 = E_e(m_1)$، $c_2 = E_e(m_2)$، ....، $c_i = E_e(m_i)$ حيث $m \in M$ ، $c \in C$، $e,d \in K$، فعليه أن يقوم باستنتاج إمّا كهدف نهائي m_i، m_1، m_2،....، m_i أو كهدف وسيط d أو خوارزمية بديلة من أجل استعادة m_{i+1} من $c_{i+1} = E_e(m_{i+1})$.

يُعدّ هجوم النص المعمّى فقط (بالنسبة إلى محلل التعمية) أضعف هجوم؛ لأنه يتضمن امتلاك المهاجم للنص المعمّى فقط، وفي المقابل، تُعدّ خوارزميات وخطط التعمية التي ينجح كسر تعمية النصوص المعمّاة بها عن طريق هذا الهجوم ضعيفة جدًّا.

---

(1) كتاب (المدخل إلى علم التعمية)، تأليف: ساري خالد، 2015م.

(2) ثمة حالات ليست فيها خوارزمية التعمية معلومة للمهاجم، تتجسّد مثل هذه الحالات كثيرًا في المعمّيات الكلاسيكية.

وينجح هذا الهجوم عند حصول المهاجم على النص الواضح m للنص المعمّى c؛ أي عند توصّله للهدف النهائي، ويُعدّ ناجحًا بنسبة أكبر إذا استطاع المهاجم استنتاج المفتاح d أو اكتشاف خوارزمية بديلة.

إنَّ لموضوع هجوم النص المعمّى فقط تشعّبات عدة، فمثلًا لو كان النص المعمّى الذي يمتلكه المهاجم ذا قيمة لاكتفى فقط باستعادة النص الواضح المقابل بوصفه هدفًا نهائيًّا دون الحاجة إلى اكتشاف المفتاح d، أمّا لو كان النص المعمّى مجرد وسيلة (أي ليس ذا قيمة) لكانَ على المهاجم دراسة خصائصه من أجل استعادة النص الواضح المقابل، ولكن ليس كهدف نهائي إنما من أجل إيجاد طريقة لاستنتاج المفتاح والاستفادة منه لفك تعمية رسائل مستقبلية معمّاة به، أو ابتكار خوارزمية ما لاستعادة أي نص واضح من نص معمّى دون الحاجة حتى إلى معرفة المفتاح، وبمجمل الأحوال، يعتمد الهدف النهائي لهجوم النص المعمّى فقط على رغبة محلل التعمية.