الجمهورية العربية السورية

وزارة التعليم العالي والبحث العلمي

جامعة تشرين

كلية الهندسة الميكانيكية والكهربائية

قسم هندسة الاتصالات والإلكترونيات

دراسة أعدت لنيل الإجازة

في هندسة الاتصالات والإلكترونيات:

دراسة زيادة تعقيد خوارزمية RSA

باستخدام الأعداد النتروسوفية

إعداد الطالب:

علي عامر الوف

إشراف الدكتور المهندس:

هيثم الرضوان

العام الدراسي:

2023-2022

الملخص:

الهدف من هذه الورقة العلمية هو بناء النسخة النيوتروسوفية من خوارزمية التشفير RSA، حيث نستخدم أسس نظرية الأعداد النيوتروسوفية المتكاملة مثل دالة فاي أويلر النيوتروسوفية، والأعداد الصحيحة النيوتروسوفية، والتطابقات النيوتروسوفية لبناء خوارزمية جديدة للتشفير تعتمد على خوارزمية RSA الشهيرة. في هذا البحث قدمنا لأول مرة النسخة النتروسوفية من الخوارزمية RSA بالاعتماد على أسس نظرية من نظرية الأعداد النتروسوفية الموضوعة لأول مرة عام 2021، وقد أظهرنا كفاءة النسخة المطورة من خلال توضيح العديد من الجداول والأمثلة ذات الصلة.

الفهرس

الفصل الأول

1.1 مقدمة:

يعتبر التشفير من أهم الأدوات التي تستخدم في عالم الحوسبة والاتصالات الحديثة، حيث يساعد على حماية البيانات الحساسة والمعلومات الخاصة من الوصول غير المصرح بها. ويتم ذلك عن طريق تحويل البيانات النصية إلى صيغة مشفرة غير قابلة للقراءة إلا بواسطة الأطراف المصرح لها فقط.

تعتمد خوارزميات التشفير على استخدام مفاتيح سرية تمكن من فك تشفير البيانات المشفرة، وتتضمن هذه المفاتيح مفتاح التشفير ومفتاح فك التشفير. ومن بين أهم خوارزميات التشفير المستخدمة حاليًا هي خوارزمية RSA، والتي تعتبر من أكثر الخوارزميات أمانًا وشهرة في عالم التشفير.

2.1 التشفير والسرية:

تتمثل المهمة الأساسية والكلاسيكية للتشفير في توفير السرية من خلال طرق التشفير، الرسالة المراد نقلها يمكن أن تكون نص أو بيانات رقمية أو برنامج قابل للتنفيذ أو أي نوع آخر من المعلومات يسمى النص الصريح.[10]

تقوم أليس بتشفير النص الصريح M وتحصل على النص المشفر C إلى بوب.

يعيد بوب النص المشفر بواسطة إجرائية فك التشفير إلى النص الصريح، لفك التشفير يحتاج بوب إلى معلومات سرية هي مفتاح فك التشفير السري.

مع ذلك لا يزال بإمكانه اعتراض الرسالة، فيجب أن يضمن التشفير السرية والمنع من استخلاص أي معلومات عن النص العادي من النص المشفر.

عملية التشفير هي عملية قديمة جداً، على سبيل المثال تم تقديم تشفير قيصر منذ أكثر من 2000 عام مضت

توفر كل طريقة تشفير الخوارزمية E وخوارزمية فك التشفير D.

في طرق التشفير الكلاسيكية تعتمد خوارزميتي التشفير وفك التشفير على نفس المفتاح K، يستخدم هذا المفتاح للتشفير وفك التشفير معاً، لذلك تسمى طرق التشفير هذه متناظرة.

على سبيل المثال، في تشفير قيصر يكون المفتاح السري هو الإزاحة 3 خانات من الأبجدية المستخدمة.

3.1 أهداف التشفير:

توفير السرية ليس الهدف الوحيد للتشفير، يستخدم التشفير أيضًا لتقديم حلول لمشاكل أخرى:

1. تكامل البيانات: يجب أن يكون متلقي الرسالة قادراً على التحقق مما إذا كان تم تعديل الرسالة أثناء الإرسال، إما عن طريق أخطاء في الإرسال أو التعديل فيها، لا ينبغي لأحد أن يكون قادراً على استبدال رسالة غير مرغوب بها ب الرسالة الأصلية أو أجزاء منها.
2. المصادقة: يجب أن يكون مستلم الرسالة قادراً على التحقق من الأصل (المعلومات المرسلة الصحيحة)، فلا ينبغي لأحد أن يكون قادراً على إرسال رسالة ل بوب والتظاهر أنه أليس.
3. عدم التنصل: يجب ألا يكون المرسل قادراً على إنكار إرساله للرسالة لاحقاً.

إذا كانت الرسائل مكتوبة على الورق، فإن الوسيط ألا وهو الورق يوفر درجة معينة من الحماية ضد التلاعب. التوقيعات الشخصية المكتوبة بخط اليد تهدف إلى ضمان المصادقة وعدم التنصل. إذا تم استخدام الوسائط الإلكترونية، الوسيط نفسه لا يوفر أي أمان على الإطلاق، لأنه من السهل استبدال بعض البايتات في رسالة أثناء إرسالها عبر شبكة حاسوبية، ويكون سهلًا بشكل خاص إذا كانت الشبكة متاحة للجمهور، مثل الإنترنت.

في حين أن للتشفير تاريخ طويل، نتجت الحاجة إلى تقنيات توفر سلامة البيانات والمصادقة عن الزيادة السريعة أهمية الاتصالات الإلكترونية. [10]

هناك طرق متماثلة (symmetric) بالإضافة إلى طرق عامة (public-key) لضمان النزاهة من الرسائل. تتطلب الطرق المتماثلة الكلاسيكية مفتاحًا سريًا k مشتركًا ل المرسل والمستقبل، يتم تعزيز الرسالة M بواسطة رمز مصادقة (MAC: Message Authentication code)، هذا الرمز يولد من قبل الخوارزمية المعتمدة على المفتاح المشترك.

الرسالة المدمجة (m, MAC (k, m)) تكون محمية ضد التعديلات، قد يختبر المستقبل سلامة الرسالة الواردة له عن طريق التحقق من كون:

$$MAC(k, m) = \overline{m}$$

تتطلب التوقيعات الرقمية أساليب وطرق المفتاح العمومي (public key)، كما هو الحال مع التوقيعات الكلاسيكية المكتوبة بخط اليد، فإن الغرض منها هو توفير المصادقة وعدم التنصل.

إن عدم التنصل هو ميزة لا غنى عنها إذا تم استخدام التوقيعات الرقمية لتوقيع العقود الرقمية. تعتمد التوقيعات على المفتاح السري للموقع التي يمكن إنشاؤها فقط من طرفه. من ناحية أخرى، يمكن لأي شخص التحقق مما إذا كان التوقيع صحيحًا أم لا، من خلال تطبيق خوارزمية تحقق معروفة للعامة، والتي تعتمد على المفتاح العمومي للموقع.

إذا أرادت أليس التوقيع على الرسالة M فهي تطبق خوارزمية التوقيع مع مفتاحها السري وتحصل على التوقيع

[10]. Sign(sk,m)

يتلقى بوب توقيعاً للرسالة M، ويمكنه التحقق بعد ذلك عن طريق اختبار إذا كان:

$$Verify(pk, s, m) = ok, ok: Alice\ public\ key$$

من الشائع عدم التوقيع على الرسالة نفسها، ولكن لتطبيق التشفير تابع وحيد الاتجاه أولاً ثم القيام بالتوقيع على قيمة الناتجة.

في طرق ك الخوارزمية الشهيرة جداً RSA والتي سيمت تيمناً باسم مخترعيها: Rivest, Shamir, Adleman

يتم استخدام خوارزمية فك التشفير لإنشاء التوقيعات ويتم استخدام خوارزمية التشفير للتحقق منها، وهذا النهج للتوقيعات الرقمية هو لذلك غالبًا ما يشار إليه باسم نموذج "التجزئة ثم فك التشفير".

تعتمد التوقيعات الرقمية على الرسالة. تؤدي الرسائل المختلفة إلى توقيعات مختلفة، وهكذا مثل رموز مصادقة الرسائل الكلاسيكية، فإن الرقمية يمكن أيضًا أن تستخدم التوقيعات لضمان سلامة الرسائل.

4.1 الهجمات:

الهدف الأساسي من التشفير هو الحفاظ على سرية النص العادي من الهجمات التي تحاول الحصول على بعض المعلومات حول النص العادي. كما نوقش من قبل، قد يكون الخصوم نشطين أيضًا ويحاولون تعديل الرسالة.

من المتوقع أن يضمن التشفير سلامة الرسائل، على الرغم من كون المهاجمين لهم وصول كامل إلى قناة الاتصال.

تحليل التشفير هو علم دراسة الهجمات ضد التشفير، قد تؤدي الهجمات الناجحة إلى استعادة النص الصريح (أو ل الأجزاء من النص الصريح) واستخلاصها من النص المشفر، أو استبدال أجزاء من النص الأصلي، أو تزوير التوقيعات الرقمية.

غالبًا ما يكون علم التشفير وتحليل التشفير يندرجان تحت مصطلح التشفير الأكثر عمومية.

تم تعريف الفرضيات الأساسية في تحليل الشيفرات لأول مرة من قبل كريكوف في أواخر القرن التاسع عشر، ويشار إليه بمبدأ كريكوف وينص على أن المهاجم يعرف كل تفاصيل نظام التشفير، بما في ذلك الخوارزميات وتطبيقاتها. وفقًا لهذا المبدأ، فإنه يجب أن يعتمد أمن نظام التشفير بالكامل على المفاتيح السرية لدى كل من المرسل والمستقبل.

تحاول الهجمات على المعلومات المشفرة بطريقة تشفير معينة الحصول على النصوص الصريحة المرسلة، أو بشكل أكثر حدة للحصول على المفتاح السري.

بشكل بسيط قد يكون الهجوم هجوم سلبي مقتصر على الحصول على الرسالة المرسلة ولا يحاول تعديلها، بل فقط مراقبة قناة الاتصال، لذلك فإن هذا الهجوم قد يكون غرضه الثانوي بعد اعتراض النص المشفر، القدرة على تشفير وفك تشفير الرسائل. من دون الحصول على معلومات عن المفتاح. على سبيل المثال.

تعتمد الهجمات المحتملة على الموارد الفعلية للمهاجم وعادة ما يتم تصنيفها على النحو التالي:

1. هجوم نص مشفر فقط: يكون للمهاجم القدرة الحصول على النصوص المشفرة فقط، وهذا من المحتمل أن يكون هو الحال في أي حالة تشفير، حتى لو لم يستطع المهاجم تنفيذ الهجمات الأكثر تعقيداً التي ستذكر أدناه، فهو قادر على الحصول على النص المشفر بأي طريقة تشفير، لا يمكن أن يقاوم هجوم النص المشفر فقط فهو غير آمن تماماً.
2. هجوم نص عادي معروف: يكون للمهاجم القدرة على الحصول على النص الصريح من النص المشفر، باستخدام المعلومات من أزواج النص المشفر والنص الصريح وتحليلها لمحاولة فك تشفير الملف المشفر، فإن تكرار أنماط مشفرة تسهل تحليلها وبالتالي كسر التشفير.
3. هجوم مختار بنص عادي: يمتلك المهاجم القدرة على الحصول على النصوص المشفرة معينة للحصول منها على نصوص صريحة معينة، ومن ثم يقوم المهاجم بالتعديل على المعلومات وترسلها بقصد فك التشفير للنظام ككل، هذا النوع من الهجمات يفترض أنه يجب على المهاجم الحصول على زوج من النص المشفر والنص العادي له ثم تقوم بتحليلها دون أي تفاعل إضافي.

4. هجوم نص عادي تم اختياره بشكل متكيف: هذا النوع من الهجمات يشابه النوع السابق ولكن يقوم المهاجم ببعض التحليلات على أزواج النصوص العادية والمشفرة وبالتالي الحصول على مزيد من الأزواج وإجراء تحليل أكثر وهذا يعني وصول أطول لجهاز التشفير واستخدامه بشكل متكرر.

5. هجوم النص المشفر المختار بشكل متكيف: هذا النوع من الهجمات على غرار هجمات النص العادي أعلاه، يمكن أن يختار المهاجم النصوص المشفرة ويحصل على النصوص الصريحة المقابلة، في هذا النوع من الهجمات المهاجم بشكل فعلي له القدرة على الوصول لجهاز فك التشفير فعلياً.

5.1 أمن يمكن إثباته:

من المستحسن تصميم أنظمة تشفير آمنة بشكل إثباته، إثبات الأمان يعني أن البراهين الرياضية تظهر أن نظام التشفير يقاوم أي نوع من الهجمات. تم القيام بعمل رائد في هذا المجال من قبل شانون في نظريته الرياضية للاتصالات، طور شانون مقاييس رياضية لكمية المعلومات المرتبطة برسالة ومفهوم السرية التامة.

يقاوم التشفير السري تماماً جميع الهجمات على النص المشفر فقط، المهاجم في هذه الحالة لا يحصل على أي معلومات على الإطلاق عن النص العادي، حتى لو كانت موارده من قدرة ووقت غير محدودة. قد تتأثر الطريقة التي يتم بها الهجوم على طريقة التشفير بأحداث عشوائية، لذلك يتم استخدام الخوارزميات الاحتمالية لنمذجة المهاجمين.[10]

يعتمد أمن نظام التشفير بالمفتاح العام على صلابة بعض القضايا الحسابية (لا توجد خوارزميات فعالة لحل هذه المشكلة)، على سبيل المثال، يمكن أن تكون المفاتيح السرية لخوارزمية RSA سهلة الكشف ما إذا كان حساب العوامل الأولية لعدد صحيح كبير ممكنًا.

ومع ذلك، يُعتقد أن تحليل الأعداد الصحيحة الكبيرة أمر غير ممكن لا توجد براهين رياضية لصلابة القضايا الحسابية المستخدمة في أنظمة المفاتيح العامة. لذلك فإن البراهين الأمنية لأساليب المفتاح العام هي

دائمًا ما تكون مشروطة، فهي تعتمد على صحة الافتراض الأساسي للخوارزمية المستخدمة أي البناء الرياضي.

ينص الافتراض عادة على أن دالة معينة f هي تابع باتجاه واحد، بمعنى أن التابع f يمكن حسابه بكفاءة، ولكن من غير المجدي حساب $f(x)$ من x.

يمكن جعل هذه الافتراضات، بالإضافة إلى فكرة الدالة أحادية الاتجاه، اصطلاحات غاية في الأهمية ودقيقة عن طريق استخدام خوارزميات متعددة الحدود الاحتمالية. إن احتمالية عكس الدالة بنجاح بواسطة خوارزمية متعددة الحدود الاحتمالية صغير جداً بشكل مهمل.

بالتالي فإن الدوال أحادية الاتجاه ليست فقط المكونات الأساسية لتشفير المفتاح العام والتوقعيات الرقمية، بل هي تعبر عن إتقان حسابي متقن لمولدات بت شبه عشوائية كما سيتبين في هذا البحث لاحقاً.

إذا كان f دالة وحيدة الاتجاه مثلما ذكرنا مسبقاً، فهي ليست كذلك فقط أي أنه من المستحيل حساب xمن $f(x)$،

لكن هناك بعض البنات من النص الرقمي تسمى (hard-core bits) من المعلومات الأصلية x يصعب استنتاجها، وهذه الميزة تسمى بت الأمن لدالة أحادية الاتجاه.

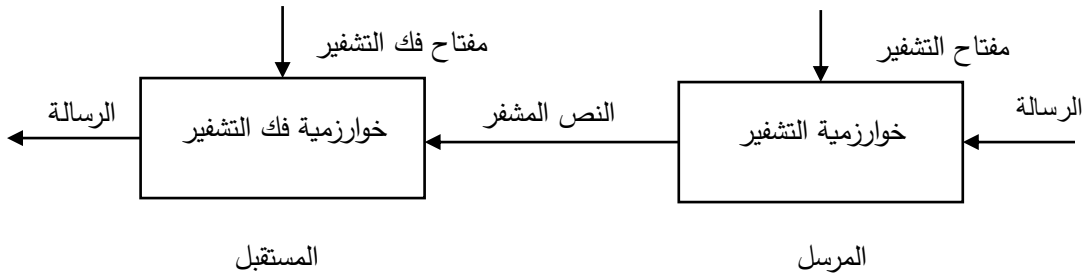
على سبيل المثال البت الأقل أهمية هو بت hard-core لدالة RSA من أجل $x \to x^e \ mod \ n$ ، بدءًا من بذرة عشوائية، فإنه بتطبيق f مرارًا وتكرارًا وأخذ الجزء البتات ذات الخاصية hard-core في كل خطوة، نحصل بالنتيجة على تسلسل بت شبه عشوائي، ولا يمكن تمييز تسلسلات البت هذه من تسلسلات البت العشوائية حقاً المولدة بواسطة خوارزمية توليد عشوائي فعالة أو أي مكافئ لها.

6.1 خوارزميات التشفير:

تستخدم خوارزميات التشفير لتحويل البيانات إلى نص مشفر تعتمد هذه الخوارزميات على مفتاح التشفير لتغيير البيانات بطريقة يمكن التنبؤ بها أي بحيث يمكن إعادتها إلى نص عادي باستخدام مفتاح فك التشفير، على الرغم من ان البيانات المشفرة ستظهر بشكل عشوائي، وهناك أنواع مختلفة من خوارزميات التشفير المصممة لتناسب مختلف الأنظمة.

وتعرف خوارزميات التشفير أيضاً بأنها مجموعة من المعادلات الرياضية المعقدة والتي يتم استعمالها حالياً في مجال الحوسبة الرقمية في العديد من المجالات المختلفة وذلك من أجل توفير حماية أكبر للمعلومات على شبكة الانترنت بصفة خاصة.

يظهر الشكل أدناه وصف تخطيطي لاستخدام أحد أنظمة التشفير لحماية رسالة منقولة:



الشكل 1-1: نظام اتصالات بين مرسل ومستقبل يظهر فيه استخدام التشفير لحماية الرسالة المرسلة

تقسم خوارزميات التشفير المستخدمة في أنظمة الاتصالات والمعلومات الحديثة إلى:

- خوارزميات التشفير المتناظر.
- خوارزميات التشفير غير المتناظر.

- **خوارزميات التشفير المتناظر(Symmetric-Key Encryption) :**

يوفر تشفير المفتاح المتماثل أو المتناظر السرية عند الإرسال بين طرفين، باعتبار أليس وبوب هما المرسل والمستقبل، لا ينبغي للمهاجم الذي يعترض رسالة بينهما الحصول على أي معلومات مهمة حول محتواها.

لإنشاء قناة اتصال آمنة، يتفق أليس وبوب أولاً على مفتاح k، يحتفظون بمفتاحهم المشترك k سرًا.
قبل إرسال الرسالة M إلى بوب تقوم أليس بتشفير M باستخدام خوارزمية التشفير المتناظر والمفتاح k، تحصل على النص المشفر: $c = E(k, m)$ وترسل الرسالة المشفرة c ل بوب.
باستخدام خوارزمية فك التشفير D ونفس المفتاح k يقوم بوب بفك تشفير الرسالة c لاستعادة المعلومات الأصلية الصحيحة: $m = D(k, m)$.

نحن ندعو هذا التشفير بالتشفير المتناظر أو المتماثل، لأن كلا أجزاء الاتصال المرسل والمستقبل تستخدم نفس مفتاح التشفير k للتشفير وفك التشفير، وتكون خوارزميتي التشفير E وفك التشفير D معروفة من الطرفين.

يمكن لأي شخص يملك مفتاح التشفير فك تشفير الرسالة المرسلة المشفرة بهذه الخوارزميات.

بالتالي يجب أن يبقى المفتاح k سرياً، وتتمثل إحدى المشكلات الأساسية في التشفير المتناظر في كيفية اتفاق أليس وبوب على مفتاح سري مشترك k بطريقة آمنة وفعالة.

ونتيجة لهذه المفارقة ظهرت الحاجة إلى أساليب تشفير المفتاح العام، والتي سوف نناقشها تباعاً.[10]

تعريف 1: تتكون طريقة التشفير بالمفتاح المتناظر من:

$$E: K \times M \rightarrow C$$

$$E_k: M \rightarrow C, m \rightarrow E(k, m)$$

حيث:

العناصر $m \in M$ هي النصوص الصريحة (وتسمى أيضاً بالرسائل).

C هي النصوص المشفرة.

العناصر $k \in K$ هي المفاتيح.

E_k هي دالة التشفير المرتبطة بالمفتاح k.

D_k هي الدالة العكوسة ك وظيفة والمقابلة ل E_k، هي دالة فك التشفير، يفترض أن توجد خوارزميات فعالة لحساب D_k و E_k.

يتم تشارك المفتاح بين طرفي الاتصال مثلما ذكرنا، ويحتفظ كلا الطرفين به بشكل سري حرصا على سلامة المعلومات المرسلة. والشرط الأساسي المهم لطريقة التشفير E هو التشفير باستخدام المفتاح k دون إمكانية الحصول عليه عند الهجوم، فيكون من المستحيل فك التشفير ب طريقة فك التشفير D دون امتلاك المفتاح.

من أكثر خوارزميات التشفير بالمفتاح المتناظر هي: DES, AES.

من بين جميع خوارزميات التشفير، فإن خوارزميات التشفير المتناظر لديها أسرع زمن تطبيق وتنفيذ في الأجهزة والبرمجيات، لذلك هي مناسبة جداً لتشفير كميات كبيرة من البيانات.

إذا كان كل من أليس وبوب يريدان استخدام نظام تشفير بالمفتاح المتناظر، فعليهم أولاً تبادل المفتاح السري.

لهذا يجب عليهما استخدام قناة اتصال آمنة، وغالبا ما تكون الطريقة لتبادل المفتاح هي طريقة المفتاح العام التي سنأتي بذكرها لاحقاً.

أنظمة تشفير المفتاح العام أقل كفاءة وبالتالي فهي غير مناسبة لكميات كبيرة من البيانات، وبالتالي فإن تشفير المفتاح المتماثل وتشفير المفتاح العمومي يكملان بعضهما البعض لتوفير نظام تشفير عملي.

في خوارزميات التشفير المتناظر نميز بين نوعين من الخوارزميات وطرق التشفير، وهي: stream ciphers, block ciphers.

يقوم التشفير الكتلي (block cipher) بمعالجة النصوص الصريحة ذات الطول الثابت، بينما يقوم تشفير الدفق (stream cipher) بمعالجة تدفقات النص الصريح محرف بمحرف أي طول الكتبة هنا بطول محرف.

تعريف 2: تشفير الدفق

لنفترض أن K مجموعة المفاتيح المتناظرة وأن M مجموعة النصوص الصريحة، تبعاً لهذا السياق ستسمى عناصر M بالمحارف، فيكون:

$$E^*: K^* \times M^* \rightarrow C^*, E^*(k, m) := c := c_1 c_2 c_3 \dots$$

تشفر السلسلة أو الدفق: $m := m_1 m_2 m_3 \dots \epsilon M^*$ من أحرف النص الصريح بالشكل:$c :=$ $c_1 c_2 c_3 \dots \epsilon C^*$ كمحارف من النص المشفر باستخدام سلسلة المفاتيح: $k := k_1 k_2 k_3 \dots \epsilon K^*$.

يتم تشفير التسلسل $m := m_1 m_2 m_3$ محرف بمحرف لهذا الغرض تعمل طريقة التشفير كما يلي، تقوم بتشفير محارف النص العادية m_i بالمفتاح المقابل لها k_i:

$$c_i = E_{ki}(m_i) = E(k_i, m_i), i = 1,2, \dots$$

عادة ما تكون المحارف في M وC وK هي خانات ثنائية أو بايتات.

بالطبع يجب أن يكون تشفير محارف النص العادي باستخدام k_i أمراً متكيفاً، من أجل سهولة فك التشفير وفعاليته في المستقبل، ويتم ذلك أيضا محرفاً بمحرف من خلال تطبيق الخوارزمية D بنفس تسلسل المفاتيح: ... $k_1 k_2 k_3$ التي تم استخدامها للتشفير، فيكون:

$$c = c_1 c_2 c_3 \dots \rightarrow D(k, c) := D_{k1}(c_1) D_{k2}(c_2) D_{k3}(c_3) \dots$$

تأتي الحاجة إلى تشفير الدفق من الآتي، على سبيل المثال من نظام ما نحصل على تدفقات في الخرج والدخل بالطبع، ويجب أن يظل التدفق الرئيسي في تشفير الدفق سراً، إنه ليس بالضرورة أن يكون المفتاح السري الذي يتم مشاركته بين أطراف الاتصال، لأنه قد يتم إنشاء تدفق المفاتيح من المفتاح السري المشترك بواسطة ملف مولد شبه عشوائي كما سيذكر أدناه.

ملاحظة: في معظم شيفرات الدفق يكون المعامل الثنائي XOR للبتات $a, b \epsilon \{0,1\}$ ، باعتبار قيمة فعلية حقيقية تم تطبيقها، نعلم أن: $a\ XOR\ b = 1, if\ a = 0, b = 1\ or\ a = 1, b = 0$، و $a\ XOR\ b = 0, if\ a = 0, b = 0\ or\ a = 1, b = 1$.

أخذ عدم تكافؤ بتين a, b يعني جمعهما مع باقي القسمة على 2، بمعنى $a\ XOR\ b = a + b\ mod\ 2$.

كممارسة شائعة نحن نرمز ل بوابة عدم التكافؤ بالرمز أو المعامل $\oplus$،أي:

$$a \oplus b \coloneqq (a_1 XOR b_1)(a_2 XOR b_2)(a_3 XOR b_3) \dots (a_n XOR b_n).$$

تعريف 3: التشفير الكتلي

التشفير الكتلي هي طريقة تشفير متناظر يكون فيه: $M = C = \{0,1\}^n$ وفضاء (مجموعة) المفاتيح $K = \{0,1\}^r$:

$$E: \{0,1\}^r \times \{0,1\}^n \to \{0,1\}^n, (k, m) \to E(k, m).$$

باستخدام مفتاح سري k بطول ثنائي r تقوم خوارزمية التشفير E بتشفير كتل النص *الصريح* m *بطول ثنائي ثابت* n

وتكون كتل النص المشفر الناتج: $c = E(k, m)$، ويكون طول الكتلة المشفرة هو: $n.n$.

تكون أطوال الكتل المشفرة بشكل نموذجي هي 64 bits كما في خوارزمية (DES)، أو 128 bits كما في خوارزمية (AES)، ويكون طول المفتاح بشكل نموذجي هو 56 bits كما في خوارزمية (DES)، وبطول 128 bits كما في خوارزمية (AES).

لنعتبر كتلة مشفرة هي E بطول n وطول المفتاح r، وهناك 2^n كتلة من النص الصريح، و 2^n كتلة من النص المشفر بطول n للكتلة. من أجل طول ثابت للمفتاح k تكون دالة التشفير:

$$E_k: m \to E(k,m)\ \{0,1\}^n$$

عندما نختار مفتاح k من r-bits ل تابع التشفير E، فيكون k هو مجموعة من المفاتيح من: $\{0,1\}^r$.

من هذه الاعتبارات، نستنتج أنه لا يمكننا الحصول على المثالية في التشفير مع السرية التامة عند التطبيق، كما ذكرنا سابقاً في تشفير البت بسرية تامة.[10]

- **خوارزميات التشفير غير المتناظر (Asymmetric-Key Encryption):**

الفكرة الأساسية لتشفير المفتاح العام هي مفهوم المفاتيح العامة، مفتاح كل شخص ينقسم إلى جزأين: مفتاح عمومي للتشفير متاح للجميع ومفتاح سري لفك التشفير يحتفظ به المالك سراً، سنناقش في هذا البحث مفهوم التشفير بالمفتاح العام ونذكر أهم خوارزمياته وأشهرها خوارزمية RSA مع تقديم تطوير رياضي فعلي يحسن أداء وفعالية الخوارزمية RSA كما سيذكر بالفصل القادم.[10]

تعريف 1: مفهوم تشفير المفتاح العام

يوفر التشفير المتماثل الكلاسيكي قناة اتصال آمنة لكل زوج من المستخدمين، من أجل إنشاء مثل هذه القناة، يجب على المستخدمين الاتفاق على مفتاح سري مشترك. بعد إنشاء اتصال آمن بالقناة يمكن ضمان سرية الرسالة. التشفير المتماثل يتضمن أيضًا طرقًا للكشف عن التعديلات في الرسائل وطرق تحقق من أصل الرسالة، وبالتالي تكون السرية والأمان أنجزت باستخدام تقنيات المفتاح السري.

ومع ذلك، يجب استخدام تقنيات المفاتيح العمومية للتوزيع الآمن للمفاتيح السرية، وعلى الأقل بعض الأشكال المهمة للمصادقة وعدم التنصل تتطلب أيضًا أساليب المفتاح العام، مثل التواقيع الرقمية.

يجب أن يكون التوقيع الرقمي هو النظير الرقمي للتوقيع المكتوب بخط اليد، ويجب أن يعتمد التوقيع على الرسالة المراد توقيعها والمعروفة فقط للموقّع، يجب أن يكون الطرف الثالث (المهاجم المتنصت على القناة) غير قادرًا على التحقق التوقيع.

في طرق تشفير المفتاح العام، لا يقوم طرفا الاتصال بمشاركة مفتاح سري sk، ولكن كل مستخدم لديه زوج من المفاتيح: مفتاح سري معروف فقط له ومفتاح عمومي pk معروف للجميع.

لنفترض أن بوب لديه زوج المفاتيح (sk, pk)، وأليس تريد تشفير رسالة m وإرسالها ل بوب، فمثل أي شخص آخر تعرف أليس المفتاح العام ل بوب، تحسب أليس الرسالة المشفرة: $c = E(pk, m)$، عن طريق تطبيق دالة التشفير E مع فتاح بوب العمومي pk.

كما سبق نشير إلى التشفير بمفتاح ثابت pk بواسطة E_{pk}، بمعنى $E_{pk}(m) = E(pk, m)$.

ومن هذا نستطيع استنتاج أن نظام التشفير سيكون آمناً فقط إذا كان من غير الممكن حساب الرسالة m من $c = E(pk, m)$.

ولكن كيف يمكن لبوب بعد ذلك استعادة الرسالة m من النص المشفر c؟ هنا يظهر استخدام مفتاح بوب السري

sk.

يجب أن تمتلك دالة التشفير E_{pk} على الخاصية التي تسهل الحصول على الرسالة m من النص المشفر $c = E(pk, m)$، باستخدام مفتاح بوب السري sk، لأنه هو الشخص الوحيد الذي يمكنه فك تشفير الرسالة.

حتى أليس التي قامت بتشفير الرسالة m، لن تكون قادرة على الحصول على m من $c = E(pk, m)$ إذا فقدت هي الرسالة m!

بالطبع يجب أن توجد خوارزميات فعالة لأداء التشفير وفك التشفير، سنلخص متطلبات تشفير المفتاح العام تباعاً.

أي نحن نبحث عن عائلة من الدوال $(E_{pk})_{pk \epsilon PK}$، بحيث تكون كل دالة E_{pk} قابلة للحساب بواسطة خوارزمية فعالة. أي يكون حساب غير عملي حساب الصورة المسبقة للدالة E_{pk}، مثل هذه العائلات من الدوال $(E_{pk})_{pk \epsilon PK}$ تسمى دوال أحادية الاتجاه (one-way functions).

تدل PK على مجموعة المفاتيح العامة المتاحة لكل دالة (إجرائية) من عائلة الدوال E_{pk}، لكل دالة E_{pk} من عائلة الدوال يجب أن يكون لها معلومات سرية هي المفتاح السري sk، يجب الحفاظ على هذا المفتاح سرياً مما يتيح إجراء عمليات حسابية عكوسة فعالة عن استقبال الرسالة المشفرة، هذه المعلومات السرية تسمى trapdoor information، وتسمى الدوال وحيدة الاتجاه مع هذه الخاصية ب trapdoor function.

في عام 1976، نشر كل من W. Diffie و M.E. Hellman ورقة بحثية سميت ب "الاتجاهات الجديدة في التشفير" كان محتواها التشفير بالمفتاح العام وآليته، قدموا طريقة المفتاح العمومي للاتفاق على المفتاح المرسل والتي هي قيد الاستخدام حتى يومنا هذا.

بالإضافة إلى ذلك، وصفوا كيف ستكون التوقيعات الرقمية وآلية العمل بها، واقترحا كسؤال مفتوح البحث عن مثل هذه الدوال للتشفير بالمفتاح العام.

أول نظام تشفير حقق آلية التشفير بالمفتاح العام والتوقيع الرقمي كان RSA cryptosystem المنشور عام 1978 من قبل كل من رايفست وشامير وآدلمان ([RivShaAdl78]).

سميت الخوارزمية RSA تيمناً بمخترعيها: R. Rivest, A. Shamir and L. Adleman، يوفر التشفير وفق RSA cryptosystem التشفير والتوقيع الرقمي وهو نظام التشفير بالمفتاح العام الأكثر شيوعاً واستخداماً حتى يومنا هذا.

تستند الخوارزمية لصعوبة تحليل الأعداد الأولية الكبيرة، مما يتيح تكوين دوال أحادية الاتجاه ذات الخاصية trapdoor، إحدى الميزات الآخرى للدوال أحادية الاتجاه هو صعوبة استخراج اللوغاريتمات المتقطعة، وهذه القضايا من نظرية الأعداد هي أسس معظم أنظمة تشفير المفتاح العام المستخدمة اليوم.

يحتاج كل مشارك في نظام تشفير المفتاح العام إلى مفتاحه الخاص k، حيث $k = (sk, pk)$، يتكون من جزء عام وجزء خاص.

لضمان أمن نظام التشفير، يجب أن يكون من غير المجدي وغير الممكن حساب المفتاح السري sk من المفتاح العام pk، ويجب أن يكون من الممكن اختيار المفاتيح k بشكل عشوائي من فضاء كبير من البارمترات المتاحة، يجب أن تتيح الخوارزمية الفعالة مثل هذا الأداء ل الاختيار العشوائي.

بفرض أن بوب هو أحد المشتركين في تطبيق يستخدم التشفير بالمفتاح العام، يختار بوب بشكل عشوائي مفتاحه:$k = (sk, pk)$، يحافظ بوب على سرية المفتاح sk ويتيح المفتاح pk، والآن يمكن لجميع مشتركي التطبيق استخدام pk لتشفير الرسائل المرسلة ل بوب.

لمناقشة الفكرة الأساسية للتواقيع الرقمية، لنفترض أنه لدينا عائلة الدوال $(E_{pk})_{pk \epsilon PK}$، يمكن استخدام هذه العائلة من الدوال ذات الخاصية trapdoor للتواقيع الرقمية، لنفترض أن pk هو المفتاح العام ل أليس، لحساب المعكوس E_{pk}^{-1} ل E_{pk}، المفتاح السري ل أليس يكون مطلوباً.

لذا تكون أليس هي الوحيدة القادرة على فعل هذا، إذا أرادت أليس التوقيع على رسالة m تقوم بحساب $E_{pk}^{-1}(m)$

وتأخذ هذه القيمة كتوقيع رقمي s للرسالة m، يمكن للجميع التحقق من توقيع أليس باستخدام المفتاح العام ل أليس وحساب $E_{pk}(s)$.

إذا كان $E_{pk}(s) = m$، يكون واضحاً ل بوب أن أليس وقعت الرسالة لأن أليس فقط من تستطيع حساب $E_{pk}^{-1}(m)$.

من التطبيقات المباشرة الهامة لأنظمة تشفير المفتاح العام هي توزيع مفاتيح الجلسات، مفتاح الجلسة هو يستخدم في أنظمة التشفير الكلاسيكية لتشفير رسائل جلسة اتصال واحدة.

إذا كانت أليس تعرف المفتاح العام لبوب، فقد تنشئ جلسة مفتاح، وتقوم بتشفيره باستخدام مفتاح بوب العمومي وإرساله إلى بوب.

التوقيعات الرقمية تُستخدم لضمان أصالة المفاتيح العامة عن طريق مؤلفي الشهادات، يوقع المرجع المصدق المفتاح العام لكل مستخدم معه المفتاح السري.

يمكن التحقق من التوقيع بالمفتاح العام ببروتوكولات التشفير لمصادقة المستخدم، هذه المفاهيم اليوم هي أساسية للاتصال عبر الإنترنت والتجارة الإلكترونية.

يعد تشفير المفتاح العام مهمًا أيضًا لعلم الحاسب النظرية، تم تطوير نظريات الأمان والتأثير على نظرية التعقيد بتقدم علوم نظرية الأعداد....

7.1 قضايا رياضية:

في هذا القسم نقدم لمحة موجزة عن العمليات الحسابية المعيارية الضرورية لفهم الخوارزميات المدروسة في هذا الفصل والفصل القادم.[10]

تعريف 1: الأعداد الصحيحة:

نفترض أن $\mathbb{Z}$ تشير إلى مجموعة الأعداد المرتبة $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$، عناصر $\mathbb{Z}$

ندعوها بالأعداد الصحيحة. جميع الأعداد الصحيحة الموجبة الأكبر من 0 تدعى بالأعداد الطبيعية $\mathbb{N}$.

العمليتين $n + m$ الجمع و $n \times m$ الضرب هي عمليات معرفة، إن عمليتي الضرب والجمع تلبي بديهيات الحلقة التبادلية مع عنصر الوحدة. ندعو $\mathbb{Z}$ بحلقة الأعداد الصحيحة.

الجمع والضرب والرفع الأس. توجد خوارزميات فعالة لجمع وضرب الأعداد، الخوارزميات الفعالة يتم تقييد وقت تشغيلها بواسطة كثير حدود يكون حجمه بحجم مدخلات الخوارزمية.

حجم الرقم هو طول ترميزه الثنائي، بمعنى إن حجم $n \epsilon \mathbb{N}$ يساوي إلى $\log_2(n) + 1$، ويتم الإشارة إليه كما يلي $|n|$.

بفرض $a, b \epsilon \mathbb{N}$، و $a, b \leq n$ و $k := \lfloor \log_2 n \rfloor$، إن عدد عمليات الحساب للبت بالنسبة ل $a + b$ هو $O(k)$، ومن أجل عملية الضرب $a \times b$ هو $O(k^2)$.

إن عملية الضرب يمكن تحسينها إلى $O(k \log_2(k))$ إذا تم استخدام خوارزمية الضرب السريع.

طريقة التربيع المتكرر تؤدي إلى خوارزمية فعالة في حساب a^n، وهي تتطلب على الأكثر $2 \times |n|$.

مثلاً نحسب a^{16} كما يلي $((((a^2)^2)^2)^2)$، وهي عبارة عن أربع عمليات تربيع، وهنا تظهر الفعالية مقارنة مع النقيض من 15 عملية ضرب ضرورية للطريقة التقليدية.

القسمة مع باقي. إذا كان m وn عددان صحيحان، $m \neq 0$، تكون عملية قسمة n بواسطة m، نستطيع كتابة $n = q \times m + r$ بطريقة فريدة من هذا القبيل: $0 \leq r < abs(m)$.

نحن ندعو q بحاصل القسمة، وr باقي القسمة، وغالباً ما نشير إلى r ب $a \bmod b$.

العدد الصحيح m يقسم عددًا صحيحًا n إذا كان n مضاعفًا لـ m، بمعنى: $n = mq$ حيث أن q هو عدد صحيح، نقول عن m هو قاسم أو عامل ل n.

القاسم المشترك الأعظم $\gcd(m, n)$ لعددين $m, n \neq 0$، بأنه عدد أكبر عدد صحيح موجب يقسم كل من m وn.

يتم تعريف $\gcd(0,0)$ على أنه صفر، وإذا كان $\gcd(m, n) = 1$ ندعو كل من m وn بأنهما أوليان فيما بينهما.

تحسب الخوارزمية الإقليدية القاسم المشترك الأكبر لعددين اثنين وهي من أقدم الخوارزميات في الرياضيات، كما يلي:

الخوارزمية الإقليدية. تحسب الخوارزمية الإقليدية القاسم المشترك الأعظم لعددين: a, b، $\gcd(a, b)$

حيث أن: $a \neq 0, b \neq 0$، وتنتهي الخوارزمية لأن العدد غير السالب r يتناقص في كل خطوة، وسيكون $\gcd(a, b)$ ثابت في الحلقة، وهذا لأن: $\gcd(a, b) = \gcd(b, a\ mod b)$.

في الخطوة الأخيرة يصبح الباقي r مساوي للصفر ونحصل على: $\gcd(a, b) = \gcd(a, 0) = abs(a)$.

int gcd $(int\ a, b)$

1) $while\ b \neq 0\ do$
2) $\quad r \leftarrow a\ mod\ b$
3) $\quad a \leftarrow b$
4) $\quad b \leftarrow r$
5) $return\ abs(a)$

الأعداد الأولية والعوامل. نقول عن عدد طبيعي p أنه عدد أولي إذا كانت قواسمه هي العدد 1 والعدد p نفسه.

إذا كان العدد $n \in \mathbb{N}$ عدد غير أولي فإننا ندعو هذا العدد بعدد مركب (composite)، الأعداد الأولية هي صلب وأساس إعداد أنظمة التشفير بالمفتاح العام.

الأعداد الصحيحة للقياس n. بفرض n عدد صحيح موجب، وبفرض a وb عددان صحيحان، عندها نستطيع القول أن a يطابق b للقياس n، وتكتب كما يلي: $a \equiv b\ mod\ n$، إذا كان a وb يتركان نفس الباقي نفسه عند القسمة على n، أو إذا كان n يقسم دون باقي $a - b$، وبالتالي هي علاقة تكافؤ.

أنظمة البواقي. كما أوضحنا سابقاً أن علاقة التطابق للقياس n هي علاقة تكافؤ على المجموعة $\mathbb{Z}$، وحيث أن كل علاقة تكافؤ تجزئ المجموعة المعرة عليها إلى فصول أو صفوف تكافئ (Equivalent classes). إذاَ:

$$\mathbb{Z}/\equiv_n = \{[a] | a \epsilon \mathbb{Z}\}$$

هي تجزئة للمجموعة $\mathbb{Z}$، لكن فصل التكافؤ $[a]$ والذي يحول العنصر a هو:

$$\bar{a} = [a] = \{b\epsilon\ \mathbb{Z} | b \equiv a\ mod\ n\}$$

وعليه إذا رمزنا للمجموعة: $\mathbb{Z}/\equiv_n$ بالرمز $\mathbb{Z}_n$، نجد أن $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ والتي تسمى مجموعة البواقي للقياس n (Residue classes)، وعندما $n = 4$، نجد أن:

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$$

حيث: $[0] = \{0, \pm 4, \pm 8, \dots\}, [1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$.

دالة أويلر Euler phi function

دالة أويلر $\phi(n)$ هي عدد الأعداد الصحيحة الموجبة الأقل من أو تساوي n والأولية نسبياً مع n.

أي أن: $\phi(n) = |\{m\epsilon\mathbb{Z} | 1 \leq m \leq n, (m, n) = 1\}|$.

مثال: $\phi(4) = \{1,3\} = 2, \phi(9) = \{1,2,4,5,7,8\} = 6$.

مبرهنة:

إذا كان $a > 1, n > 1$ عددين صحيحين وكان $a^n - 1$ عدداً أولياً، فإن $a = 2$ و n عدد أولي.

<u>البرهان:</u>

بما أن $a^n - 1 = (a-1)(a^{n-1} + \dots + a + 1)$، إذاً عندما $a > 2, n > 1$ نجد أن $a - 1 > 1$ و

$a^{n-1} + \dots + a + 1 > a + 1 > 3$، وعليه فإن $a^n - 1$ ليس أولياً وهذا خلاف للفرض، هذا يقتضي: $a = 2$.

والآن لنفترض أن $2^n - 1$ عدد أولي وأن n ليس أولياً، إذاً $n = rs$، $1 < r < n, 1 < s < n$ حسب ما ذكر ببراهين سابقة، وعليه فإن $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1$ عدد أولي. لكن حسب ما تم إثباته أعلاه أنه إذا كان $a^n - 1$ عدداً أولياً، فإن $a = 2$.

إذاً $2^r = 2$، وعليه فإن $r = 1, s = n$ بالتالي n غير مركب، إذا n عدد أولي.

8.1 الخوارزمية RSA:

في عام 1978 قدم رون ريفيست، وآدي شامير، وليونارد آدلمان خوارزمية تشفير، والتي جاءت لتحل محل خوارزمية المكتب الوطني للمعايير (NBS) الأقل أماناً.

كان أكثر ما يميز هذه الخوارزمية تحقيقها لنظام التشفير بالمفتاح العام إضافة إلى التوقعيات الرقمية، كانت هذه الخوارزمية مستوحاة وملهمة من فكرة كل من ديفي وهيلمان من عدة سنوات خلت، حيث أنهما وصفا فكرة الخوارزمية ولكن لم يتم تطويرها حقاً.

تم تقديم هذه الخوارزمية في الوقت الذي كان من المتوقع أن يظهر فيه البريد الإلكتروني قريباً، حققت RSA فكرتين مهمتين:

1) التشفير بالمفتاح العام: هذه الفكرة تغفل الحاجة إلى "ساعي" لتسليم المفاتيح إلى المستلمين عبر قناة آمنة قبل إرسال الرسالة الأصلية. في هذه الخوارزمية يكون مفتاح التشفير عاماً في حين أن مفتاح فك التشفير ليس كذلك، لذلك يمكن فقط للشخص الذي يملك مفتاح فك التشفير الصحيح فك تشفير الرسالة المرسلة. كل شخص لديه مفاتيح التشفير وفك التشفير الخاصة به.
يجب أن تولد المفاتيح بطريقة يصعب ويستحيل معرفة مفتاح فك التشفير من مفتاح التشفير.

2) التوقيع الرقمي: قد يحتاج مستلم الرسالة إلى التحقق من أن الرسالة المرسلة له مصدرها بالفعل من المرسل (التوقيع أو الموقع)، أي وسيلة مصادقة.
يتم ذلك باستخدام فك التشفير الخاص بالمرسل، ويمكن لأي شخص لاحقاً التحقق من التوقيع، باستخدام المفتاح العام المقابل. لذلك لا يمكن تزوير التوقيع وأيضاً لا يمكن لأي أحد أن ينكر توقيعه. هذا ليس مفيدًا فقط للبريد الإلكتروني، ولكن للمعاملات الإلكترونية وعمليات الإرسال الأخرى، مثل تحويلات أموال.

إن أمان الخوارزمية RSA محقق حتى الآن، وذلك لعدم وجود محاولات ناجحة لكسر الخوارزمية حتى الآن، ويعود هذا بالغالب لصعوبة تحليل العدد الكبير: $n = pq$ لعوامله الأولية، حيث أن p و q عددين أوليين.

- **أنظمة تشفير المفتاح العام:**

يملك كل مستخدم إجرائية التشفير وفك التشفير الخاصة به، E وD، مع المفتاح العام المعلن للجميع والمفتاح الخاص الذي يبقى سرياً، وتكون إجرائيات التشفير وفك التشفير مرتبطة بالمفاتيح، والتي تكون في RSA عبارة عن مجموعات من رقمين مميزين.

نبدأ بالطبع بالرسالة نفسها، التي يرمز إليها بـ M، والتي يراد تشفيرها، هناك أربع إجرائيات ضرورية وأساسية لنظام التشفير بالمفتاح العام:

a) يمنح فك تشفير الرسالة المشفرة الرسالة الأصلية على وجه التحديد:
$$D(E(M)) = M.$$
b) عكس الإجرائية يعطي M أيضاً:
$$E(D(M)) = M.$$
c) كل من E وD سهلة الحساب.

d) كون الإجرائية E سرية لا تضر بسرية D، مما يعني أنه لا يمكن بسهولة معرفة D من E.

مع وجود E، ما زلنا لا نمنح طريقة فعالة لحساب D، إذا كان النص المشفر $C = E(M)$، فإن معرفة D بمحاولة معرفة M من $E(M)$ هو أمر غاية في الصعوبة والتعقيد، لأن عدد الرسائل المراد اختبارها سيكون كبيرة من الناحية العملية.

إن الإجرائية E تحقق كل من (a)،(c)، (d) مما سبق أي يطلق عليها: trap-door one-way function، وهي كذلك لأنه من السهل حساب المعكوس D في حالة توفر معلومات معينة، ولكنها صعبة بخلاف ذلك، أي أنه من السهل الحساب باتجاه واحد، ومن الصعب والمستحيل الحساب بالاتجاه المعاكس. أي

إن العملية ك تبديل لأنها تحقق (b) مما سبق، وهذا يعني أن كل نص مشفر هو رسالة محتملة، وكل رسالة هي نص مشفر لرسالة أخرى، والعبارة (b) مما سبق هي في الواقع تحقق غاية التوقيع الرقمي.

نناقش كل ما سيقترح ونتكلم عنه تباعاً بناء على المحددات التالية، لنفرض مستخدمين اثنين A وB أليس وبوب في نظام تشفير بالمفتاح العام، بحيث مفاتيح أليس وبوب هي: E_A, E_B, D_A, D_B.

- **السرية:**

التشفير، الذي أصبح الآن طريقة منتشرة في كل مكان لضمان تسليم رسالة بشكل خاص وآمن، يجعل المتطفل غير قادر على تجاوز النص المشفر.

وبالتالي فإن RSA هي إجابة رائعة لهذه المتطلبات، يمكن أن يكون معيار NBS مفيدًا فقط إذا كانت خوارزمية أسرع من RSA، عندها تستخدم RSA فقط لنقل المفاتيح بشكل آمن.

يجب أن تكون طريقة الحساب الفعالة لـ D موجودة، وذلك لجعل RSA قائمة بحد بذاتها وموثوقة تمامًا، ولكي تكون موثوقة يجب استخدام حسابات خوارزمية بسيطة، والتي هي أحد المتطلبات مما سبق تحديداً (c) مما سبق.

الآن، بفرض يريد بوب إرسال رسالة خاصة إلى أليس، سوف يستخدم بوب الإجرائية E_A لتشفير الرسالة M كما يلي $C = E_A(M)$، وبعد ذلك تقوم أليس بفك تشفير الرسالة باستخدام الإجرائية D_A، وهي فقط من يستطيع القيام بذلك، تبعاً للخاصية (d) مما سبق، وهي تسطيع الرد على بوب باستخدام E_B.

لذلك كل ما هو مطلوب هو موافقة المستخدم على أن يكون جزءًا من نظام التشفير عن طريق وضع بيانات التشفير الخاصة بهم في ملف عام. من دون الحاجة لاتصال مسبق، أيضًا بسبب الخاصية (d)، لا يمكن لأي متنصت أن يستنتج D من الاستماع إلى E.

- **التوقيع:**

للتأكيد الكامل على أن الرسالة نشأت من مرسل، ولم يتم إرسالها من خلاله فقط من قبل طرف ثالث ربما استخدم نفس مفتاح التشفير (مفتاح جهاز الاستقبال)، نحتاج إلى رقم رقمي التوقيع لتأتي مع الرسالة.

هذا له آثار واضحة ذات أهمية في تطبيقات الحياة الواقعية.

يريد بوب إرسال رسالة خاصة إلى أليس، لتوقيع الوثيقة، نستخدم حيلة صغيرة ذكية، على افتراض أن خوارزمية RSA سريعة وموثوقة، ويرجع ذلك في الغالب إلى الخاصية (c).

نقوم بفك تشفير رسالة بمفتاح بوب، المسموح به بواسطة الخاصيتين (a) و(b)، التي تؤكد أن كل رسالة هي نص مشفر ل رسالة أخرى، وأن كل نص مشفر يمكن تفسيره على أنه رسالة مشفرة، وذلك بالصيغة:

$$D_B(M) = S$$

ثم نقوم بتشفير S بمفتاح تشفير Alice: $E_A = (S) = E_A(D_B(M))$.

بهذه الطريقة، يمكننا أن نؤكد أنها وحدها القادرة على فك تشفير المستند، وعندما تفعل ذلك تحصل على التوقيع بواسطة: $D_A(E_A(D_B(M)) = S$.

إنها تعرف الآن أن الرسالة جاءت من بوب، لأن مفتاح فك التشفير فقط يمكن أن يحسب التوقيع.

لا يلزم إرسال الرسالة بشكل منفصل، حيث يمكن لأليس استنتاجها من ملف التوقيع نفسه باستخدام مفتاح التشفير المتاح للجمهور الخاص بـ Bob، $E_B(S) = E_B(D_B(M)) = M$.

بما أن إرسال S يعتمد على M، ويعتمد الإرسال المشفر الذي أرسله بوب على S، لدينا إرسال هذا يعتمد على كل من الرسالة والتوقيع، لذلك يمكن استنتاج كلاهما من المستند المرسل.

لذا لا تمتلك أليس فقط دليلًا على أن بوب وقع على الرسالة وأرسلها بالفعل، ولكنها أيضًا لا يمكن تعديل M ولا يمكن تزوير توقيع لأي رسالة أخرى.

الآن لنفرض أن "دخيلاً" حاول الكذب وأعلن أنه من الملف العام؟ هذه ليست مشكلة في RSA، حيث يتم استخدام "التوقيعات" للتحقق. يحتاج التوقيع فقط إلى التأكيد على أنه جاء من الملف العام (PF) بحد ذاته، وفي كل مرة ينضم فيها مستخدم إلى شبكة، يحصل الجميع على نسخة مرسلة بأمان من آخر تحديث للملف العام، المخزن على نظامهم، ولن يضطروا أبدًا إلى البحث عنها.

أي شخص يحاول إرسال رسالة والتظاهر بأنه في الملف العام لن يحمل التوقيع المناسب، وسيتم تمييزه على أنه "متسلل"، كما أنه لن يستقبل أي إعلام من الملف العام لأنه لم ينضم إليها أبدًا.

- **التطبيقات والتنبؤات والتنفيذ على العتاد:**

للخوارزمية تطبيقات في تحويل الأموال الإلكترونية أيضًا، يجب أن تكون المعلومات المالية آمنة، ويمكن توقيع الشيكات إلكترونيًا باستخدام RSA، يجب اتخاذ مزيد من التدابير، مثل تنفيذ أرقام شيك فريدة تسمح بالتحقق من هذا الرقم المعين القابل للتحويل / الصرف، في الواقع، يمكن تطبيق مثل هذا النظام على أي نظام إلكتروني يحتاج إلى نظام تشفير مُنفّذ.

في بحثهم RSA لعام 1978، توقع مؤلفو RSA تطور عالم بريد إلكتروني آمن ولـ RSA لتشفير محادثة هاتفية حية. الآن هذه الأشياء هي بالفعل جزء من الحياة اليومية بسبب RSA.

يجب ألا يكون جهاز التشفير هو المخزن المؤقت المباشر بين المحطة وقناة الاتصال. بدلاً من ذلك، يجب أن يكون روتينًا فرعيًا للأجهزة يمكن تنفيذه حسب الحاجة، لأنه قد يحتاج ليتم تشفيرها / فك تشفيرها بعدة تسلسلات مختلفة من المفاتيح، وذلك لضمان مزيد من الخصوصية والمزيد من التوقيعات.

- **البناء الرياضي للخوارزمية:**

حتى الآن، أظهرنا أن كل من E وD تحسب بسهولة من خلال عمليات رياضية بسيطة، يجب أن نمثل الآن

الرسالة عدديًا، حتى نتمكن من إجراء هذه الخوارزميات الحسابية عليها.

الآن دعنا نمثل M بعدد صحيح بين 0 و$n-1$، إذا كانت الرسالة طويلة جدًا، فطبعاً نقوم بتقسيمها وتشفيرها بشكل منفصل، لتكن e,d,n أعداد صحيحة موجبة، مع (e,n) كمفتاح تشفير، و (d,n) مفتاح فك التشفير، تحسب n، كما يلي $n=pq$.

نقوم بتشفير الرسالة برفعها ل الأس e للقياس n، فنحصل على C الرسالة المشفرة، ثم يكون فك التشفير ل C عن طريق رفع C ل الأس d للقياس n.

بصيغة رياضية نحصل على خوارزميتي التشفير وفك التشفير من خلال العلاقات الرياضية الآتية:

$$C \equiv E(M) \equiv M^e \ (mod\ n) \qquad (1-1)$$

$$M \equiv D(C) \equiv C^d (mod\ n) \qquad (2-1)$$

مع ملاحظة أننا نشفر ونفك تشفير نفس كمية المعلومات، وذلك لأن كل من M وC هي أعداد صحيحة بين 0 و$n-1$، وبسبب كون التطابق معياري.

الآن يأتي السؤال عن إنشاء مفتاح التشفير نفسه، أولاً نختار عددين p,q أوليين نضرب العددين وينتج $n=pq$. بالرغم من كون n عاماً، فإنه من المستحيل معرفة p,q لأنه من المستحيل تحليل n إلى عواملها الأولية. وبالتالي من المستحيل عملياً اشتقاق d من e.

الآن للحصول على كل من e و d، نختار d ليكون عدداً صحيحاً كبيراً، والذي يجب أن يكون عدد أولي نسبي بالنسبة ل $(p-1)(q-1)$. بمعنى أنه يجب أن تتحقق المعادلة التالية:

$$\gcd\big(d,(p-1)\cdot(q-1)\big)=1.$$

الآن نستطيع حساب e من d، حيث أن e هو المعكوس الضربي ل d، هذا يعني أنه يجب أن تتحقق العلاقة التالية:

$$e\cdot d=1\big(mod\phi(n)\big). \qquad (3\text{-}1)$$

هنا نقدم دالة فاي ل أويلر $\phi(n)$، ناتج فاي أويلر هو عدد الأعداد الصحيحة الموجبة الأقل من n وهي أولية نسبياً مع n.

بالنسبة لأي عدد أولي p يكون من الواضح أن $\phi(p)=p-1$، بحيث تكون خصائص الدالة فاي:

$$\begin{aligned}\phi(n)&=\phi(p)\cdot\phi(q)\\&=(p-1)\cdot(q-1)\\&=n-(q+p)+1. \qquad (4\text{-}1)\end{aligned}$$

من المعادلات السابقة نستطيع استنتاج:

$$e\cdot d\equiv 1(mod\ \phi(n)) \qquad (1\text{-}5)$$

وتكون هذه المعادلة مكافئة ل المعادلة:

$$e \cdot d = k \cdot \phi(n) + 1 \qquad (6-1)$$

حتى الآن ما سبق نستطيع أن نشير إلى العلاقات التالية بأنها علاقات صحيحة:

$$D\big(E(M)\big) \equiv (E(M))^d \equiv (M^e)^d \ (mod\ n) = M^{e \cdot d} \ (mod\ n)$$
$$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e \ (mod\ n) = M^{e \cdot d} \ (mod\ n)$$

أيضاً، نظراً لأن $e \cdot d = k + \phi(n) + 1$، يمكننا استبدال المعادلات أعلاه والحصول على:

$$M^{e \cdot d} \equiv M^{k \cdot \phi(n)+1} \ (mod\ n).$$

من الواضح أننا نريد جعل المعادلة السابقة تساوي M، لإثبات ذلك سنستخدم خواص فاي أويلر وفيرما، من أجل أي عدد صحيح M أولي نسبيا ل n، لدينا:

$$M^{\phi(n)} \equiv 1 \ (mod\ n).$$

نظراً لأننا حددنا مسبقاً أن $0 \leq M < n$، نحن نعلم أن M لن تكون أولية نسبياً مع n إلا إذا كانت M إما p أو q، من الأعداد الصحيحة في هذا المجال، لذلك هناك فرصة كبيرة لحدوث هذا وأن تكون M إما p أو q لها نفس الحجم ك $2/n$.

هذا يؤدي إلى أن M ستكون أولية نسبياً مع n، وبالتالي سيكون:

$$M^{e \cdot d} \equiv M^{k \cdot \phi(n)+1} \equiv (M^{\phi(n)})^k M \equiv 1^k M \ (mod\ n) = M.$$

- **عمليات تشفير وفك تشفير فعالة:**

حسب مؤلفي خوارزمية RSA فإن حساب M^e، يتطلب على الأكثر $2 \cdot \log_2 e$ عملية ضرب، و $2 \cdot \log_2 e$ عملية قسمة، وذلك إذا استخدمنا الإجراء أدناه، من المهم بالنسبة لنا معرفة عدد الخطوات المطلوبة لجهاز كمبيوتر لتشفير الرسالة حتى نتمكن من معرفة ما إذا كانت الطريقة سريعة وفعالة أم لا.

a) ليكن $e_k e_{k-1} \dots e_1 e_0$ التمثيل الثنائي ل e.

b) نسند للمتغير C للقيمة 1.

c) نكرر الخطوات التالية من أجل: $i = k, k-1, \dots, 0$

نسند ل C لباقي قسمة C^2/n، وإذا كان $e_i = 1$ نسند ل C قيمة باقي قسمة $C \cdot M$ على n.

d) تتوقف الخوارزمية، والآن C هو الشكل المشفر ل M.

هناك إجراءات أكثر فاعلية، لكن هذا الإجراء جيد أيضا، حيث يتبع فك التشفير نفس الإجراء المماثل للتشفير، يمكننا تنفيذ العملية بأكملها على عدد قليل من الشرائح الإلكترونية المدمجة.

- **إيجاد e, d**

حساب d سهل جداً، نريد فقط إيجاد عدد d أولي نسبي بالنسبة ل $\phi(n)$، فيكون أي عدد أولي أكبر من $\max(p, q)$ مناسب كقيمة ل d.

لإيجاد e نستطيع استخدام تغيير أو (تفريع) من خوارزمية إقليدس لحساب القاسم المشترك الأكبر ل d و $\phi(n)$.

نحسب السلسة: $x_0, x_1, x_2, \dots$، حيث أن $x_0 \equiv \phi(n), x_1 = d, \dots, x_{i+1} \equiv x_{i-1} (mod\ x_i)$، ويستمر الحساب حتى نصل ل $x_k = 0$، عندها سيكون: $\gcd(x_0, x_1) = x_{k-1}$.

الآن نوجد الأعداد a_i, b_i بحيث $x_i = a_i \cdot x_0 + b_i \cdot x_1$، وإذا كان x_{k-1} عندها سيكون b_{k-1} هو المعكوس الضربي ل $x_1 (mod\ n)$، وعلى وجه التحديد نحصل على e، وبحيث $k < 2 \log_2 n$ فإن الحساب سيكون سريعاً وفعالاً.

- **مثال تطبيقي:**

ليكن: $p = 37, q = 43, n = p \cdot q = 1591, d = 71, \phi(1591) = 1512$، عندها نستطيع حساب e بطريقتين، إما تغيير الخوارزمية الإقليدية المذكور أعلاه، أو باستخدام الخوارزمية الإقليدية الموسعة بالاستفادة من كون e هو المعكوس الضربي ل d، كما يلي:

$x_0 = 1512$	$a_0 = 1$	$b_0 = 0$
$x_1 = 71$	$a_1 = 0$	$b_1 = 1$
$x_2 = 21$	$a_2 = 1$	$b_2 = -21$
$x_3 = 8$	$a_3 = -3$	$b_3 = 64$
$x_4 = 5$	$a_4 = 7$	$b_4 = -149$
$x_5 = 3$	$a_5 = -10$	$b_5 = 213$
$x_6 = 2$	$a_6 = 17$	$b_6 = -263$
$x_7 = 1$	$a_7 = -27$	$b_7 = 575$

وبهذا نحصل على $e = 575$ وهو المعكوس الضربي ل $d = 71$ للقياس، باستخدام هذه القيمة وباقي قيمنا نبدأ الآن في التشفير. نستخدم تمثيلًا رقميًا قياسيًا إلى حد ما للأبجدية الإنجليزية: حيث نمثل الفراغ أو المسافة بين الكلمات ب 00، $A = 01, B = 02, \dots, Z = 26$. يجب أن تكون كل كتلة من الرسالة أقل من $n = p \cdot q = 1591$، في حالتنا سنقسم الرسالة إلى كتل من حرفين، لأنها لن تتجاوز 159، أي نستطيع القول أيضاً أنه كلما كانت قيم p, q أكبر استطعنا تشفير كمية معلومات في كل كتلة أكثر، سنختار الرسالة $NO\ ODD$ لتشفيرها:

ترمز هذه الرسالة إلى: 1415 0015 0404، والآن نستطيع تطبيق نسخة الخوارزمية المذكورة في هذا الفصل والتشفير على أساسها، وعلى أساس التمثيل الثنائي ل $\boldsymbol{e}$ وهو 100011111، وحسب الخوارزمية إذا كان $e_k = 1$ نربع C ونضربها ب M، وغير ذلك نربع C فقط، وأخيراً نضع الناتج للقياس n.

لنأخذ على سبيل المثال أول كتلة من $M = 1415$ ونشفرها كما يلي:

$$M^{575} = (((((((((1^2 \cdot M)^2)^2)^2)^2 \cdot M)^2 \cdot M)^2 \cdot M)^2 \cdot M)^2 \cdot M)^2 \cdot M$$
$$= 824\ (mod\ 1591)$$

أي أن أول كتلة تصبح بعد التشفير: 0824.

بشكل مشابه يمكن فك التشفير كما يلي: $824^{71} \equiv 1415 (mod\ 1591)$.

- **مدى أمان RSA:**

تعد خوارزمية RSA بالفعل من بين أقوى الخوارزميات، ولكن هل يمكن أن تصمد أمام أي شيء؟ بالتأكيد لا شيء يمكن أن يصمد أمام اختبار الزمن. في الواقع، لا توجد تقنية تشفير آمنة تمامًا من هجوم تحليل شفرات واقعي. طرق مثل هجوم الأعمى (brute-force attack) بسيط ولكنها طويلة ويمكن أن تكسر رسالة، ولكن ليس من المحتمل أن يكسر مخطط التشفير بشكل كامل. يجب علينا أيضًا التفكير في النهج الاحتمالي، بمعنى هناك دائمًا احتمال أن يحصل شخص ما على "مفتاح واحد من بين مليون". حتى الآن، لا نعرف كيف نفعل ذلك أي إثبات ما إذا كان نظام التشفير غير قابل للكسر. إذا لم نتمكن من إثبات ذلك، فسنرى على الأقل ما إذا كان هناك شخص ما يمكن كسر التشفير. هذه هي الطريقة التي تم بها اعتماد معيار NBS وRSA بشكل أساسي. على الرغم من سنوات من المحاولات، لم يُعرف أي شخص باختراق أي من الخوارزميتين، وهذه المقاومة للهجوم تجعل RSA آمنة من الناحية العملية.

سوف نرى سبب صعوبة كسر RSA بسبب صعوبة تحليل عوامل n، تحليل الأعداد الكبيرة ليس صعبًا بشكل مثبت، ولكن لا توجد خوارزميات موجودة اليوم لتحليل عدد مكون من 200 خانة بكمية معقولة من الوقت. ساهم كل من Fermat وLegendre في هذا المجال من خلال تطوير خوارزميات التحليل.

لإثبات أن RSA آمنة، سننظر في كيفية محاولة محلل التشفير الحصول على مفتاح فك التشفير من مفتاح التشفير العام، وليس كيف يحاول دخيل "سرقة" مفتاح فك التشفير. يجب الاعتناء بهذا لأن المرء يحمي أمواله، من خلال طرق الأمن المادي، يقدم مؤلفو RSA مثالاً: جهاز التشفير (والذي يمكن أن يكون على سبيل المثال، مجموعة من الشرائح المتكاملة داخل جهاز كمبيوتر) منفصل عن باقي النظام. من شأنه أن يولد مفتاح التشفير ومفاتيح فك التشفير، لكنه لن يظهر مفتاح فك التشفير، حتى بالنسبة لمالكه. في الواقع، سوف يمحو مفتاح فك التشفير إذا استشعر محاولة اقتحام.

التحليل إلى العوامل الأولية. بما أن معرفة عوامل n ستعطي $\phi(n)$، وبالتالي d، محلل الشفرات سوف يكسر التشفير إذا أخذ في الاعتبار n. ومع ذلك، فقد ثبت عمليا أن تحليل الأرقام أمر غاية في الصعوبة ومع ذلك، فإن العديد من خوارزميات تحليل العوامل موجودة. مؤلفو RSA أشاروا إلى Knuth وPollard كمصادر جيدة لمثل هذه الخوارزميات.

كما قدموا أيضاُ خوارزمية غير منشورة تعود ل Richard Schroeppel، والتي تحلل n بخطوات متقاربة دقيقة:

$$exp\sqrt{\ln n \cdot \ln\ln n} = n^{\sqrt{\ln n \div \ln\ln n}} = (\ln n)^{\sqrt{\ln n \div \ln\ln n}}$$

الجدول التالي هو الذي قدمه مؤلفو RSA في عام 1978، يفترضون إجراء عملية التحليل في خوارزمية Schroeppel تستغرق ميكرو ثانية لحساب وتقديم البيانات التالية لأطوال مختلفة من n:

عدد الخانات	عدد العمليات	الزمن
50	1.4×10^{10}	*3.9 hours*
70	9.0×10^{12}	*104 days*
100	2.3×10^{15}	$74\ years$
200	1.2×10^{23}	$3.8 \times 10^{9}\ years$
300	1.5×10^{29}	$4.9 \times 10^{15}\ years$
500	1.3×10^{39}	$4.2 \times 10^{25}\ years$

يوصي مؤلفو RSA بأن يكون طول n حوالي 200 خانة، ومع ذلك ، قد يكون طول n متغيراً بناءً على أهمية سرعة التشفير مقابل الأمان. تسمح الخوارزمية في الواقع للمستخدم (المسؤول) باختيار طول المفتاح، وبالتالي مستوى من الأمان، وهي مرونة غير موجودة في الكثير من أنظمة التشفير قبل عام 1978 (مثل طريقة NBS).

- **الهجمات على خوارزمية RSA:**

كما رأينا، فإن خوارزمية RSA هي نظام تشفير آمن للغاية تم استخدامه في الماضي ثلاثون عامًا لتوفير الأمان في ملايين التطبيقات على الإنترنت. ومع ذلك، فإن الخوارزمية عانت عددًا من الهجمات أو المحاولات الخاصة بإيجاد واستغلال نقاط الضعف في الخوارزمية. نذكر أساس أمان خوارزمية RSA كون من المستحيل تحليل n إلى القيم المقابلة q وp.

أنواع الهجمات. في كتابه عشرين عاماً من الهجمات على الخوارزمية RSA، صنف دان بونيه الهجمات إلى عدة أصناف منفصلة هي: 1 الهجمات الأولية (Elementary Attacks)، 2 الأس الخاص المنخفض (Low Private Exponent)، 3 الأس العام المنخفض (Low Public Exponent)، 4 هجمات التنفيذ أو التضمين (Implementation Attacks)، وسنتحدث في هذا البحث بشكل موجز عن هجمات التنفيذ.

هجمات التنفيذ. لا علاقة للفئة الأخيرة من الهجمات على خوارزمية RSA بمهاجمة الخوارزمية نفسها، بل ينطوي الهجوم على إيجاد نقاط ضعف في تنفيذ الخوارزمية. يُطلق على أحد أنواع هجوم التنفيذ اسم

"هجوم التوقيت" لأنه يعتمد على تحديد الوقت الذي تستغرقه لأداء فك التشفير واستخدام هذا جنبًا إلى جنب مع معلومات حول الكمبيوتر الذي تم من خلاله تنفيذ الخوارزمية لحساب قيمة d.

نشرح كيفية شن الهجوم على تنفيذ بسيط لـ RSA باستخدام "خوارزمية تكرار التربيع "، بفرض التمثيل الثنائي ل $d = d_n d_{n-1} \dots d_0$، تحسب خوارزمية تكرار التربيع النص المشفر $C = M^d \ mod \ n$ باستخدام $2n$ معامل ضرب على الأكثر، لأنه يقوم على ملاحظة أن: $C = \prod_{i=0}^{n} M^{2id_i} \ mod \ n$، تعمل الخوارزمية كما يلي:

ندع Z تساوي M و C يساوي 1، من أجل $i = 0, \dots, n$ نقوم بالخطوات:

1. إذا كان $d_i = 1$ نجعل C مساوية ل $CZ \ mod \ n$.
2. نسند ل Z ناتج $Z^2 \ mod \ n$.
3. في نهاية الخوارزمية C تكون لها القيمة $M^d \ mod \ n$.

المتغير Z سوف يأخذ مجموعة من القيم $M^{2^i} \ mod \ n$، من أجل $i = 0, \dots, n$. المتغير C "يجمع" القوى المناسبة في مجموعة القيم حتى الحصول على $M^d \ mod \ n$.

للقيام بالهجوم يطلب مارفن المهاجم الحصول على عدد كبير من التوقيعات للرسائل $M_1, \dots, M_k \ \epsilon \mathbb{Z}_N^*$، وقياس الوقت اللازم لإنشاء كل ملف توقيع. يستعيد الهجوم أجزاء من d واحدًا تلو الآخر، و بدءاً من البت الأقل أهمية. نحن نعلم أن d عدد فردي، وبالتالي $d_0 = 1$، نأخذ بعين الاعتبار فيه $Z = M^2 \ mod \ n$ و $C = M$، وبفرض كان $d_1 = 1$، تحسب الخوارزمية $CZ = M \cdot M^2 \ mod \ n$، وغير ذلك لا يتم الحساب. لنفرض أن t_i هو الزمن اللازم لحساب $M_i \cdot M_i^2 \ mod \ n$، وطبعاً هذا الزمن سيختلف تبعاً ل قيم M_i، يقوم مارفن بقياس t_i (قبل تصاعد الهجوم) بمجرد حصوله على المواصفات المادية لجهاز التشفير.

- **أهمية الخوارزمية:**

قبل ظهور الإنترنت، كان التشفير من نواحٍ عديدة يعتبر مشكلة للحكومات فقط. تم تقديم خوارزمية RSA في وقت كانت فيه الشعبية المحتملة للإنترنت أصبحت واضحة، ومع هذه الشعبية جاء ارتفاع

الطلب على القدرة على نقل المعلومات بأمان. خوارزمية RSA، التي يُنظر إليها على أنها نظام تشفير للمفتاح العام غير قابل للكسر تقريبًا، سرعان ما أصبحت الطريقة المفضلة لتشفير الإنترنت بما في ذلك تشفير البريد الإلكتروني. اليوم، يستمر استخدام RSA لتشفير رسائل البريد الإلكتروني بالإضافة إلى بروتوكول طبقة المنافذ (SSL) المستخدم في غالبية عمليات تبادل بيانات الإنترنت.

الفصل الثاني

1.2 مقدمة:

النتروسوفيا هي فرع فلسفي رياضي يتعامل مع دراسة اللاحتمية والتناقض وعدم القدرة على اتخاذ القرار، تم تطوير هذا العلم من قبل العالم فلورنتين سماركانده في التسعينات. الجبر النتروسوفي هو فرع من الرياضيات الذي يتعامل مع تطبيق المنطق النتروسوفي على الهياكل الجبرية، يتضمن دراسة النظم الجبرية التي تدمج مفهوم اللاحتمية والتناقض وعدم القدرة على اتخاذ القرار. يستخدم الجبر النتروسوفي في مختلف المجالات مثل صنع القرار والذكاء الاصطناعي والمنطق الضبابي.

2.2 قضايا وتعاريف رياضية[9] :

تعريف 1: لتكن R حلقة، I عدم التحديد ذات الخاصية $I^2 = I$، عندها $R(I) = \{a + bI; a, b \in R\}$ هي حلقة نتروسوفية. إذا كانت $R = Z$ هي حلقة الأعداد الصحيحة، عندها $Z(I) = \{a + bI; a, b \in Z\}$ هي حلقة الأعداد النتروسوفية الصحيحة، وندعو عناصر $Z(I)$ بالأعداد النتروسوفية الصحيحة.[3-8]

تعريف 2: يدعى العدد $a + bI$ عدد نتروسوفي صحيح حيث a, b عددان صحيحان حيث $I^2 = I$.

تعريف 3: يدعى $a + bI$ عدداً موجباً إذا كان: $a \geq 0$، $a + b \geq 0$، مثلاً العدد $3 - I$ موجب لأن $3 > 0$ و $3 + (-1) = 2 > 0$.

تعريف 4: يتم جمع عدديين نتروسوفيين كما يلي:

$$(a + bI) + (c + dI) = (a + c) + (b + d)I \qquad (1\text{-}2)$$

تعريف 5: يتم ضرب عدديين نتروسوفيين كما يلي:

$$(a + bI) \cdot (c + dI) = ac + adI + bcI + bdI^2$$
$$ac + I(ad + bc + bd) \qquad (2\text{-}2)$$

تعريف 6: الرفع لقوة نتروسوفية:

$$(a + bI)^{c+dI} = a^c + I[(a + b)^{c+d} - a^c] \qquad (3\text{-}2)$$

تعريف 7: القاسم المشترك الأعظم للعددين $a + bI, c + dI$:

$$\gcd(a,c) + (\gcd(a+b,c+d) - \gcd(a,c))I \qquad (4-2)$$

تعريف 8: القسمة وصيغ القسمة في $Z(I)$:

من أجل $Z(I) = \{a + bI; a, b \in Z\}$ حلقة نتروسوفية من الأعداد الصحيحة، ومن أجل أي عددين $x, y \in Z(I)$ نقول أن x/y فقط إذا وجد $r \in Z(I); r \cdot x = y$.

تعريف 9: الأعداد الأولية:

من أجل $Z(I) = \{a + bI; a, b \in Z\}$ حلقة نتروسوفية من الأعداد الصحيحة، باعتبار العنصر $x \in Z(I)$

ندعو هذا العنصر (العدد) أولي إذا $x/y \cdot z$ هذا يكافئ x/y و x/z.

تعريف 10: التطابقات:

من أجل $x = a + bI, y = c + dI, z = m + nI$ ثلاث أعداد نتروسوفية صحيحة نقول أن:

$$x \equiv y(mod z) \qquad (5-2)$$

فقط إذا كان: $z/x - y$.

3.2 لماذا الأعداد النتروسوفية الصحيحة؟[9]

الهدف الرئيس من التعمية هو إبقاء الرسائل سرية، وكما نعلم إن خوارزمية RSA تعتمد على صعوبة تحليل n إلى عواملها الأولية الكبيرة.

حلقة الأعداد النتروسوفية الصحيحة $Z(I)$ تساعد في زيادة التعقيد، وذلك لأن تحليل الأعداد النتروسوفية الصحيحة الموجبة يعد عملية أصعب بكثير. على سبيل المثال $n = 20 + 52I$ نستطيع تحليلها بعدة صيغ مختلفة كما يلي: $(4 + 2I)(5 + 7I), (4 - I)(5 + 9I), (2 + I)(18 + 14I)$ وهكذا ...، وهذا يعني إن بنينا نسخة نتروسوفية من الخوارزمية RSA، سنحصل على تعقيد أكبر يجعل أصعب فأصعب كسر الخوارزمية.

لهذا السبب نعرف صيغة نتروسوفية جديدة لتابع أويلر، والصيغة النتروسوفية الجديدة لتابع فاي تعطى كما يلي:

$$\phi(x+yI) = \phi(x)\cdot\phi(x+y); x, x+y > 0.$$

تابع فاي أويلر يعد عدد الأعداد النتروسوفية الموجبة $a+bI$ مثل $a+bI \le x+yI$ و $\gcd(a+bI, x+yI) = 1$.

وعليه توالياً نبني التعاريف والأدوات الرياضية المستخدمة بالاعتماد على دالة أويلر.

تعريف.

من أجل $x+yI$ عدد نتروسوفي موجب صحيح، نعرف الصيغة الخاصة للدالة فاي أويلر كما يلي:

$$\phi_s: Z(I) \to Z(I);\ \phi_s(x+yI) = \phi(x) + [\phi(x+y) - \phi(x)]I.$$

نظرية.

لندع $A = a+bI, M = m+nI$ عدديين نتروسوفيين صحيحين بحيث $\gcd(A, M) = 1$، عندها $A^{\phi_s(M)} = 1(mod\ M)$.

الإثبات.

$$A^{\phi_s(M)} = (a+bI)^{\phi(m)+[\phi(m+n)-\phi(m)]I}$$
$$= (a)^{\phi(m)} + I[(a+b)^{\phi(m+n)} - (a)^{\phi(m)}].$$

تبعاً للفرض، لدينا $\gcd(A, M) = 1$، وعليه فإن $\gcd(a, m) = \gcd(a+b, m+n) = 1$، وعليه فإن $(a)^{\phi(m)} = 1(mod\ m), (a+b)^{\phi(m+n)} = 1(mod\ m+n)$، هذا يقتضي:

$$A^{\phi_s(M)} = 1(mod\ m) + I[1(mod\ m+n) - 1(mod\ m)] = 1(mod\ M).$$

ملاحظة.

ليكن $x+yI, z+tI$ عديين نتروسوفيين صحيحن موجبين بحيث $\gcd(x+yI, z+tI) = 1$، عندها $\phi_s[(x+yI)(z+tI)] = \phi_s(x+yI)\cdot\phi_s(z+tI)$.

الإثبات.

$$(x + yI)(z + tI) = xz + I[(x + y)(z + t) - xz].$$

$$\phi_s[(x + yI)(z + tI)] = \phi(xz) + I[\phi[(x + y)(z + t)] - \phi(xz)]$$

$$= \big[\phi(x) + I[\phi(x + y) - \phi(x)]\big]\big[\phi(z) + I[\phi(z + t) - \phi(z)]\big] = \phi_s(x + yI) \cdot \phi_s(z + tI). \quad (6\text{−}2)$$

مثال.

بفرض $A = 3 + 2I, B = 5 + 6I$، $3 < 5{,}5 < 11$، و $gcd(3{,}5) = gcd(5{,}11) = 1$ هذا يقتضي $gcd(A, B) = 1$.

$$\phi_s(A) = \phi(3) + [\phi(5) - \phi(3)]I = 2 + [4 - 2]I = 2 + 2I.$$

$$\phi_s(B) = \phi(5) + [\phi(11) - \phi(5)]I = 4 + [10 - 4]I = 4 + 6I.$$

$$\phi_s(A \cdot B) = \phi(15) + [\phi(55) - \phi(15)]I = 8 + (40 - 8)I = 8 + 32I.$$

4.2 وصف الخوارزمية RSA النتروسوفية:[9]

بفرض طرفي الإرسال أليس وبوب، يريد بوب إرسال رسالة مؤمنة سرية ل أليس باستخدام الخوارزمية RSA المطورة، وبفرض أن النص الصريح هو $M = m + nI$، يجب على بوب أن يتبع الخطوات التالية:

الخطوة الأولى.

يختار بوب عدديين نتروسوفيين صحيحن موجبين، $p = a + bI, q = c + dI$ يحسب بوب $n = pq$ بحيث$n = pq = ac + I(ad + bc + bd)$. من الأفضل اختيار $a, a + b, c, c +$ d أربع أعداد أولية كبيرة بحيث $gcd(a, c) = gcd(a + b, c + d) = 1$.

الخطوة الثانية.

يحسب بوب $\phi_s(n) = \phi_s(p) \cdot \phi_s(q)$ بحيث:

$$\phi_s(p) = a - 1 + I[\phi(a + b) - (a - 1)] = a - 1 + I[a + b - 1 - a + 1]$$
$$= a - 1 + bI$$

$$\phi_s(q) = c - 1 + I[\phi(c+d) - (c-1)] = c - 1 + dI$$

الخطوة الثالثة.

يختار بوب عدداً نتروسوفياً عشوائياً بحيث: $e = e_1 + e_2 I$، بحيث ندعو الثنائية التي تحقق ما يلي ب $1 < e < \phi_s(n)$ $gcd\big(e, \phi_s(n)\big) = 1$، المفتاح العام $K_{pub}(e,n)$.

الخطوة الرابعة.

يشفر بوب الرسالة M كما يلي:

$$C \equiv M^e (mod\ n) = (m + nI)^{(e_1 + e_2 I)} (mod\ n)$$

$$= ((m)^{e1} + I[\big(m+n\big)^{(e_1+e_2)} - (m)^{e_1}]\big)(mod\ n) \qquad (7\text{–}2)$$

ويرسل بوب الرسالة المشفرة ل أليس.

المفتاح السري يحسب كما يلي: $e^{-1} = (e_1^{-1} + I[(e_1 + e_2)^{-1} - e_1^{-1}])\big(mod \phi_s(n)\big) =$

$$s_1 + s_2 I\big(mod\ \phi_s(n)\big).$$

وهكذا فإن أليس تفك التشفير كما يلي:

$$M \equiv C^{e^{-1}} (mod\ n) \qquad (8\text{–}2)$$

مثال.

بفرض بوب يريد إرسال الرسالة $M = 3 + 3I$ ل أليس، يختار بوب كل من $p = 3 + 2I, q = 7 + 4I$، بحيث $gcd(p,q) = 1$، وذلك لأن $gcd(3,7) = 1 = gcd(5,11) = 1$.

$$n = pq = 21 + 12I + 14I + 8I = 21 + 34I$$
$$\phi_s(n) = \phi(21) + I[\phi(55) - \phi(21)] = 12 + (40 - 12)I = 12 + 28$$

نختار e بحيث تحقق $1 < e < \phi_s(n)$، ومنه $e = 5 + 6I$، ومنه نحصل على المفتاح العام الآتي: $K_{pub} = (e,n) = (5 + 6I, 21 + 34I)$.

بوب يشفر الرسالة $M = 3 + 3I$ كما يلي:

$$C \equiv M^e(mod\ n) = (3^5 + I[6^{11} - 3^5])(mod\ 21 + 34I) \equiv 3^5(mod\ 21) + I[6^{11}(mod\ 55) - 3^5(mod\ 21)] \equiv 12 + I[6 - 12] = 12 - 6I.$$

نحسب على مفتاح فك التشفير السري كما يلي:

$$e^{-1} = 5^{-1}(mod\ 21) + I[11^{-1}(mod\ 40) - 5^{-1}(mod\ 21)] = 5 + 6I.$$

وعليه أليس تفك تشفير الرسالة المرسلة لها كما يلي:

$$M \equiv C^{e^{-1}}(mod\ n) \equiv 12^5(mod\ 21) + I[6^{11}(mod\ 55) - 12^5(mod\ 21)] = 3 + 3I.$$

نهج عمل الخوارزمية النتروسوفية على شكل كود زائف (pseudo code).

Start

|

|---------> X picks two neutrosophic positive integers P and Q

| |

| |---------> X computes N = P * Q

| |---------> X computes phi_s (N) = phi_s (P) * phi_s (Q)

| | |

| | |---------> X computes phi_s (P) = a - 1 + b * I

| | |---------> X computes phi_s (Q) = c - 1 + d * I

| |

| |---------> X picks an arbitrary neutrosophic positive integer E

| | |

| | |---------> X checks that gcd (E, phi_s (N)) = 1 and 1 < E < phi_s (N)

| |

| |---------> X calculates the public key (E, N)

|

|---------> X encrypts the text M

| |

| |---------> X calculates C ≡ M^E (mod N) using the formula

| | | C = ((m * e1) + (n * e2) * I) * (mod N)

| |

| |---------> X sends C to Y

|

|---------> Y receives C from X and decrypts the message

| |

| |---------> Y calculates M ≡ C^ (E^-1) (mod N) using the formula

| | | M = ((c * s1) + (n * s2) * I) * (mod N)

| |

|End

5.2 التوقيع الرقمي للخوارزمية النتروسوفية:[9]

بفرض طرفي الاتصال أليس وبوب، تريد أليس توقيع رسالة مرسلة منها ل بوب باستخدام الخوارزمية المطورة، تقوم أليس بالتشفير باستخدام مفتاحها الخاص، وعند استقبال بوب للرسالة المؤمنة الموقعة يستخدم مفتاح أليس العمومي، وذلك كما يلي، بفرض الرسالة المراد توقيعها $S = 2 + 6I$، وبفرض المفتاح الخاص له القيمة $d = 17 + 14I$، وبفرض أن قيمة $n = 91 + 116I$ تصبح الرسالة الموقعة المشفرة هي:

$$C \equiv S^d (mod\ n) \equiv 2^{17} (mod\ 91) + I[8^{31} (mod\ 207) - 2^{17} (mod\ 91)]$$
$$\equiv 32 + 138I$$

عند استقبال بوب للرسالة يقوم بفك تشفيرها بمفتاح أليس العام ذي القيمة $e = 17 + 134I$، كما يلي:

$$S \equiv C^e (mod\ n) \equiv 32^{17} (mod\ 21) + I[170^{151} (mod\ 55) - 32^{17} (mod\ 21)]$$
$$\equiv 2 + 6I$$

6.2 تعقيد وأمان الخوارزمية بالمقارنة مع الخوارزمية التقليدية:

الآن سوف نقارن بين الخوارزمية النتروسوفية والخوارزمية التقليدية من ناحية الزمن اللازم للكسر باستخدام هجوم أعمى (Brute-force attack): (جميع القيم في الجدول الأول محسوبة ومقدرة بالثانية): [9]

يوضح الجدول المقارنة من أجل بعض القيم الخاصة ل n، والجدول الثاني اعتماداً على حجم n.

الجدول 2.1

الخوارزمية التقليدية	الزمن	Neutrosophic RSA	الزمن
$n = 187$	0.00344800949097	$n = 187 + 726I$	0.00703191757209
$n = 913$	0.00358390808105	$n = 913 + 13128I$	0.00805377960208
$n = 14041$	0.00469871521	$n = 14041 + 542968I$	0.00614380836489
$n = 557009$	0.00167393684387	$n = 557009 + 8635898I$	0.00369000434875
$n = 9192907$	0.00201606750488	$n = 9192907 - 8635898I$	0.00369000434875

وكما نرى أن الخوارزمية Neutrosophic RSA تحتاج لزمن أعلى للكسر من الخوارزمية بمقدار الضعف.

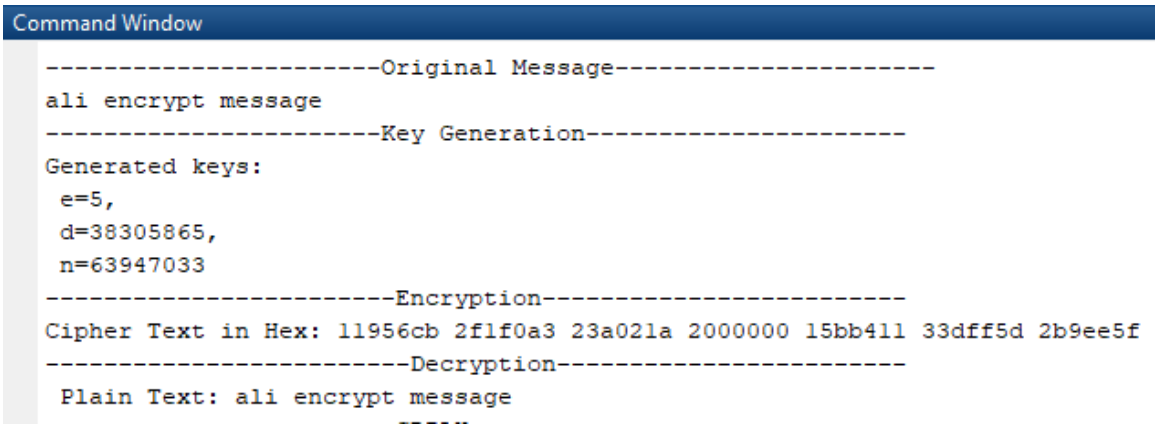
مقارنة أخرى سنقدمها اعتماداً على حجم n والهجوم الأعمى.

الجدول 2.2

الخوارزمية التقليدية	الزمن بالميلي ثانية	Neutrosophic RSA	الزمن بالميلي ثانية
The size of n is 7	0.002	Same size	0.004

The size of n is 8	0.002	Same size	0.005
The size of n is 9	0.56	Same size	1.2
The size of n is 10	4.2	Same size	8.6

نتائج المحاكاة لعدة برمجيات طبقت لتوضيح مهام التشفير وفك التشفير باستخدام الماتلاب لكل من الخوارزميتين التقليدية والمطورة النتروسوفية:

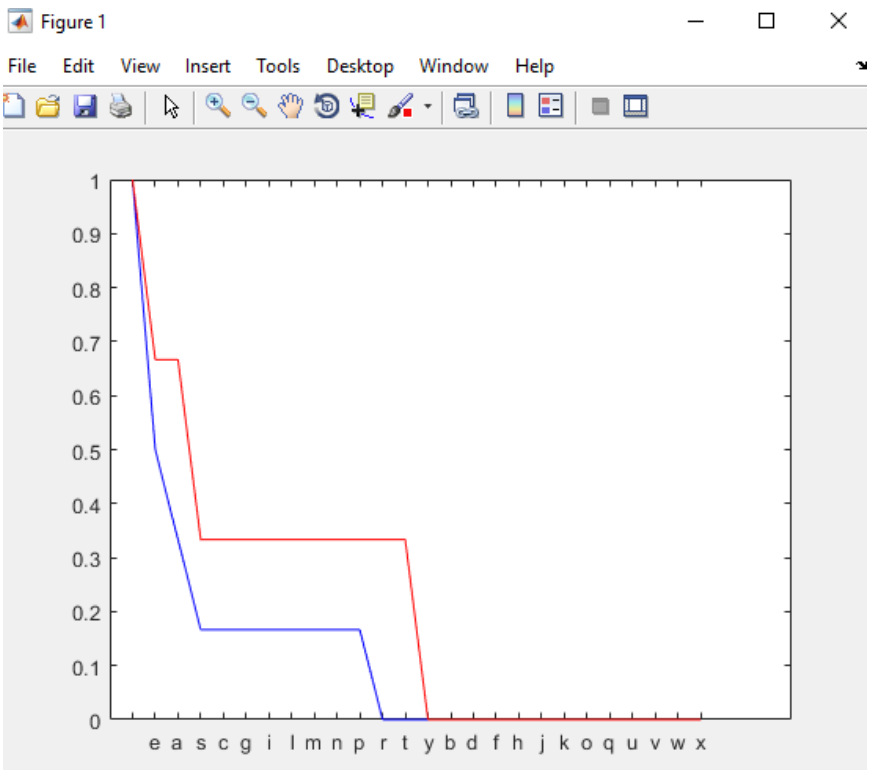


الشكل (2-1): عمليتي التشفير وفك التشفير

توضح الصورة أعلاه تشفير وفك التشفير النص الصريح ali encrypt message بالخوارزمية التقليدية بقيم المفتاح العام $K_{pub}(5, 63947033)$، وفك التشفير بالمفتاح الخاص $K_{pri}(38305865, 63947033)$، تم ترميز النص الصريح بعد عملية تشفيره بالترميز الست عشري للمحارف لزيادة الأمان.

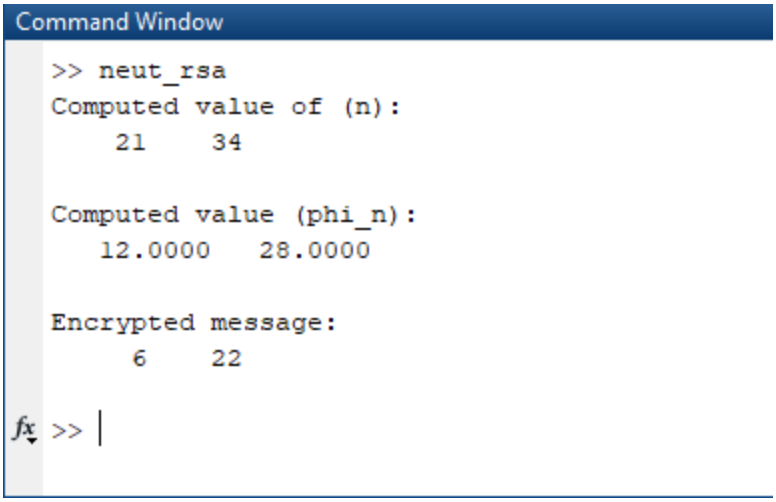
في الشكل البياني الموضح أدناه نظهر رسم التوزيع التكراري للأحرف في النص المدخل لتشفيره، والنص المشفر.

تمثل قيم المحور X الأحرف الأبجدية في النص الصريح والمشفر، والمحور Y المقيَّس يمثل تكررات استخدام المحارف بشكل مقيسّ.



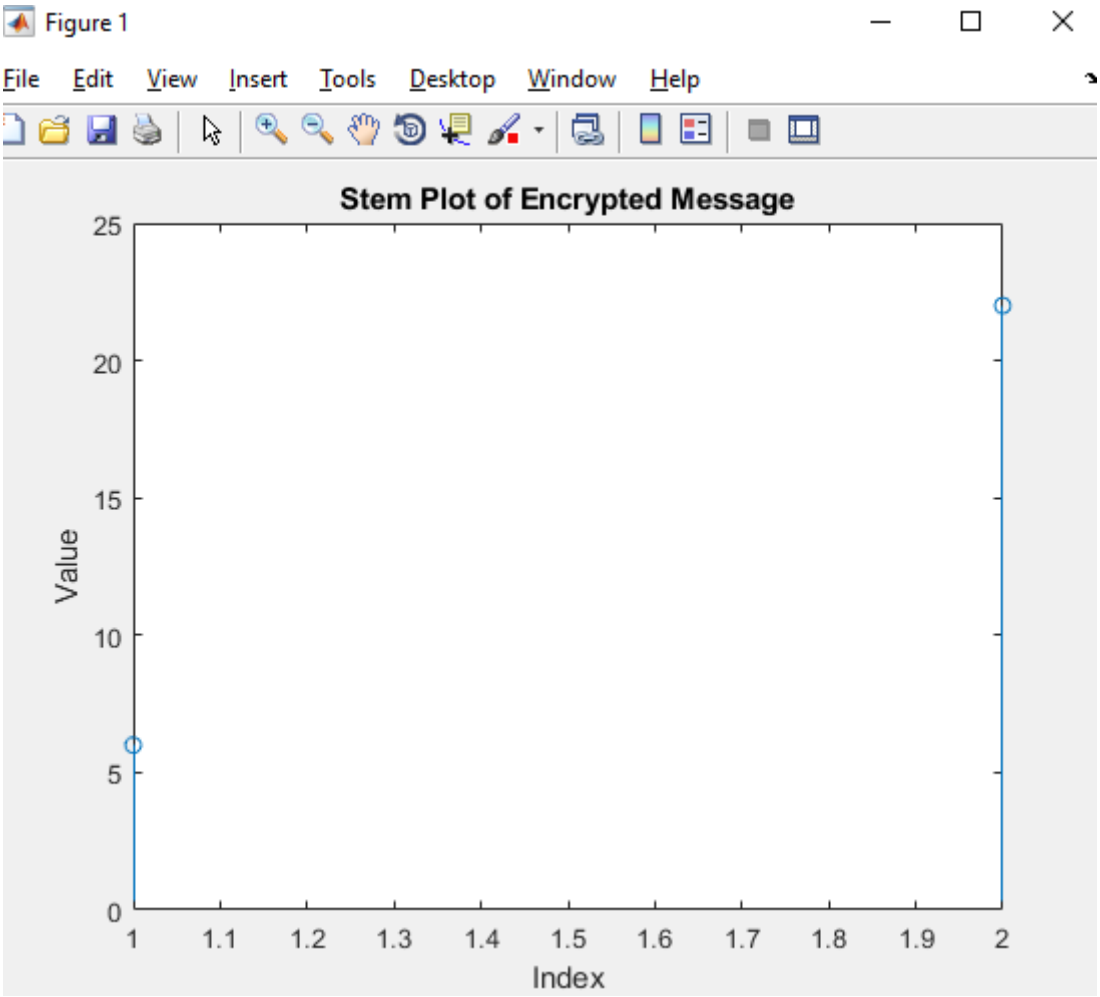
الشكل (2-2): التمثيل البياني للمحارف الأصلية والمشفرة

تظهر النتيجة التالية عملية بناء المفتاح العام واستخدامه في تشفير النص الصريح $M = 3 + 3I$، عند استخدام مفتاح نتروسوفي عام هو $K_{pub} = (187 + 25I, 21 + 34I)$:



الشكل (2-3): القيم العددية للخوارزمية النتروسوفية

في الرسم البياني التالي الموجه لإظهار نتائج متجه التشفير النتروسوفي، يمثل المحور X فهرس القيمة المشفرة الناتجة في المتجه C والمحور Y يمثل القيم المقابلة للفهارس:



الشكل (2-4): التمثيل البياني لقيم متحول الرسالة المشفرة

خاتمة:

في هذا البحث قدمنا لأول مرة النسخة النتروسوفية من الخوارزمية RSA بالاعتماد على أسس نظرية من نظرية الأعداد النتروسوفية الموضوعة لأول مرة عام 2021 من قبل الباحث محمد أبو بالا، وقد أظهرنا كفاءة النسخة المطورة من خلال توضيح العديد من الجداول والأمثلة ذات الصلة، حيث قدمنا بعض الأرقام التي أظهرت أن التعقيد ازداد بمقدار الضعف بمقارنة بالإصدار الكلاسيكي من الخوارزمية.قد يكون لنظرية الأعداد النتروسوفية تأثير كبير على التشفير، لذلك نقترح على الباحثين وضع أساس أو تحديث جديد للخوارزمية مستند إلى البحث المقال المنشور (refined neutrosophic number).

References

[1] Celik, M., and Olgun, N., "An Introduction to Neutrosophic Real Banach and Hillbert Spaces", Galoitica Journal of Mathematical Structures and Applications, 2022.

[2] Celik, M., and Olgun, N., "On the Classification of Neutrosophic Complex Inner Product Spaces", Galoitica Journal of Mathematical Structures and Applications, 2022.

[3] Abobala, M., Partial Foundation of Neutrosophic Number Theory, Neutrosophic Sets and Systems, Vol. 39, 2021.

[4] Smarandache, F., and Kandasamy, V.W.B., "Finite Neutrosophic Complex Numbers", ·Source: arXiv. 2011.

[5] Agboola, A.A.A., Akinola, A.D., and Oyebola, O.Y., "Neutrosophic Rings I", International J.Mathcombin, Vol 4, pp 1-14. 2011.

[6] Adeleke, E.O., Agboola, A.A.A., and Smarandache, F., "Refined Neutrosophic Rings I", International Journal of Neutrosophic Science, Vol. 2(2), pp. 77-81. 2020.

[7] Abobala, M., "On Some Algebraic Properties of n-Refined Neutrosophic Elements and n-Refined Neutrosophic Linear Equations", Mathematical Problems in Engineering, Hindawi, 2021.

[8] Abobala, M., On Refined Neutrosophic Matrices and Their Applications in Refined Neutrosophic Algebraic Equations, Journal of Mathematics, Hindawi, 2021.

[9] Merkepci, M., Abobala, M., & Allouf, A. (2023). The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm. Fusion: Practice and Applications (FPA), Volume (10), 02, PP.69-74.

[10] Delfs, H., & Knebl, H. (2007). Introduction to Cryptography: Principles and Applications (second Ed.). Springer-Verlag Berlin Heidelberg.