تصميم نموذج لحماية البيانات بدمج خوارزميتي AES وRSA

د.م. وضاح ملوك[1]

الملخّص

انتشرت عملية نقل البيانات انتشاراً كبيراً مع انتشار الأنظمة المتعددة التي تعمل على الشابكة (الانترنيت)، كالحوسبة السحابية وغيرها. هذه الأنظمة تحتاج إلى أنظمة حماية البيانات من أجل تأمين البيانات وحمايتها من السرقة أو التجسس، وتأمين خصوصية المستخدمين، تعدّ كل من خوارزميتي RSA (Rivest-Shamir-Adelman) وAES (Advanced Encryption Standard) الخوارزميات الأساسية لتصميم أنظمة الحماية. هَدَفَ هذا البحث إلى تصميم نموذج لحماية البيانات يعتمد على دمج الخوارزميتين السابقتين بغية الإفادة من ميزات كل منهما، والحصول على مستوى أمن أعلى.

اقترح هذا البحث خوارزمية دمج تعتمد على تقسيم حجم الملفات المراد حمايتها إلى كتل جزئية بطول 128bit وتشفير هذه الكتل بخوارزميتي RSA وAES، وقد صُمِّمَ هذا النظام وأتاح إمكانية حماية البيانات وفق خوارزمية RSA وAES وخوارزمية الدمج المقترحة، وقد قورِنَ أداء الخوارزميات الثلاث لمعرفة الزمن اللازم لإجراء التشفير، وفك التشفير لكل منها.

الكلمات المفتاحية: خوارزمية AES، خوارزمية RSA، حماية البيانات، دمج.

[1] عضو هيئة تدريسية في قسم هندسة الاتصالات، كلية الهندسة والتكنولوجيا، جامعة قرطبة الخاصة.

Designing Data Security Model Combining RSA and AES

Waddah Mallouk[(1)]

Abstract

Processing of transferring data spreaded widely with spreading the multi systems which work over the internet like cloud computing and others systems.

These systems need to security systems to protect data against steeling, spy and changing and to insurance privacy for users. RSA and AES algorithms considered the main algorithms to design security systems.

This research purposes to design model for security data depending on combining RSA and AES in parallel to benefit from the advantages of both algorithm RSA and AES and to get higher security model.

The research proposes parallel hybrid algorithm depending on segment file size into sub blocks with 128-bit size and encrypted these blocks by RSA and AES in parallel.

Proposed system is designed to give ability to protect data using RSA, AES or proposed hybrid algorithm. Performance of those three algorithms are compared to calculate time of encryption and decryption time for both of them.

Key words: RSA, AES, security data, combining.

(1) Dept. of communication Engineering, Faculty of Engineering and Technology, Cordoba Private University

1-مقدِّمة:

شهد العقد المنصرم ظهور عدد من الأنظمة الأمنية والحماية في مجال الاتصالات، التي تقوم بتطبيق إجراءات لضمان أمن المعلومات المخزنة أو المرسلة، لأنَّ التحديات الأمنية تعدّ الهاجس الذي يسعى الباحثون لإزالته من خلال تطوير أنظمة حماية داعمة لنظام الاتصال الشبكي من أجل التغلب على هذه التحديات. إذ إنَّ البيانات والمعلومات المخزنة في الشبكة الحاسوبية يمكن أن تكون ذات قيمة كبيرة بالنسبة إلى الأشخاص ذوي النيّات السيئة[1].

2-هدف البحث وأهميته:

اقتراح نموذج أمني يؤمن سرية نقل البيانات في الاتصالات الشبكية من خلال دمج خوارزميتي RSA وAES ؛بغية الإفادة من ميزات كلٍ منهما، بحيث تؤمن سرعات عالية، وتضيف صعوبات أكثر أمام المهاجمين والمخترقين لأن النص المشفر خليط من تشفيرات كل من خوارزميتي RSA وAES.

3-خطوات البحث:

a) دراسة خوارزمية RSA وتطبيقها في الاتصالات الشبكية.
b) دراسة خوارزمية AES وتطبيقها في الاتصالات الشبكية.
c) اقتراح ألية لدمج خوارزميتي AES مع RSA وتطبيقها وإيجاد نتائجها.
d) مقارنة بين خوارزميتي RSA وAES وخوارزمية الدمج المقترحة.

4-الدراسات المرجعية:

تنوعت الدراسات المرجعية في مجال دعم سرية نقل البيانات وتخزينها، فبعضها ناقش أهمية تأمين البيانات عند نقلها وبعضهم عند تخزينها، فبيّن باحثون ضرورة حماية البيانات بدمج أكثر من خوارزمية تشفير لسدّ ثغرات استخدام خوارزمية تشفير وحيدة؛ وذلك لحماية البيانات في الحكومة الالكترونية عند نقلها من السحابة وإليها [1]. واكتفى آخرون باستخدام خوارزمية تشفير متناظرة لتحقيق ذلك، إذْ صَمَّمَ الباحث نظام حوسبة سحابية عام وطَبَّقَ خوارزمية AES على الملفات من أجل اجراء عملية تخزين سرية بغية تأمين البيانات قبل نقلها [2]. وقام باحثون [3] بتطبيق خوارزمية AES المتناظرة على المنصة Heroku وهي منصة عمل متكاملة لنشر التطبيقات السحابية، فكانت النتيجة زيادة سرية البيانات في التخزين السحابي. كما طَبَّقَ الباحث [4] خوارزمية AES لحماية البيانات. في حين استخدم باحثون آخرون خوارزمية تشفير غير متناظرة [5] باقتراح تحسين على خوارزمية RSA؛ وذلك بإضافة أس ثالث إلى مفتاح فك التشفير وتكرار معادلة التشفير وكذلك في فك التشفير، مما يؤدي إلى زيادة التعقيد، ومن ثَمَّ زيادة مستوى سرية البيانات مع زيادة زمن التشفير وفك التشفير بالمقارنة مع RSA بما يتناسب مع زيادة مستوى سرية البيانات عند نقلها. كما حَسَّنَ باحثون [6] خوارزمية RSA وذلك باختيار أكثر من عددين أوليين لتوليد المفتاحين العام والسري بغية زيادة السرية من خلال قوة المفتاح بزيادة تعقيد توليد المفاتيح، ولاحظوا زيادة طفيفة في زمن التشفير وفك التشفير متوافقة مع درجة التعقيد وزيادة سرية البيانات المحققة. كما حَسَّنَ الباحثون [7] خوارزمية RSA لزيادة السرية بزيادة حجم المفتاح من خلال زيادة عدد الأعداد الأولية اللازمة لتوليد المفتاحين العام والسري لأكثر من عددين، واقترحوا طريقة جديدة لزيادة السرية وتقليل زمن التشفير وفك التشفير من خلال تقسيم النص المراد تشفيره إلى كتل بحجوم مختلفة اعتماداً على حجم المفتاح. ووجد آخرون [8] أنَّ الخوارزمية المتناظرة AES هي الأسرع والأفضل بعد أن قاموا بدراسة

أهم الخوارزميات المتناظرة وغير المتناظرة وتحليلها بغية الإفادة من المقارنة بينها لتحسين أداء كل منها. إلّا أنَّ أهم البحوث في هذا المجال اتجهت لدمج أكثر من خوارزمية؛ وذلك انطلاقاً من أهمية السرية لتأمين البيانات، وتحصينها، وتحقيق خصوصية عالية تمتاز بسرية تامة، طَبَّقَ باحثون[9] ثلاث آليات لحماية البيانات، واقترحوا بداية التوثيق والتحقق بتطبيق خوارزمية md5 (message-digest5) مشفرة بخوارزمية OTP (One-Time Password) ثم تشفير البيانات بتطبيق ثلاث خوارزميات على التسلسل RSA وBlowfish وAES، ومن ثم الآلية الثالثة التحقق من سلامة البيانات بتطبيق خوارزمية SHA2 (Secure Hash Algorithm 2) وتوصلوا بذلك إلى تحقيق سرية أفضل لحماية البيانات عند نقلها، وحقَّقَ الباحثون [10] مستوى أعلى من السرية للبيانات في أثناء نقلها، بتطبيق الخوارزميات الثلاث RSA وAES وSteganography على التسلسل، واقترح الباحثون في [11] دمج خوارزميتي تشفير مختلفتين، وهما RSA وAES على التسلسل، وذلك لتحقيق مستوى أعلى لسرية البيانات في أثناء النقل والتخزين، ووجدوا أنَّ الدمج يحقق مستوى سرية أعلى مع زيادة زمن التشفير وفك التشفير. واقترحوا اتخاذ إجراءات مستقبلية تقلل هذه الزيادة في زمن التشفير وفك التشفير، واقترح الباحثون [12] حماية البيانات عند تخزينها، وذلك باقتراح مستويات متعددة لتشفير البيانات المخزنة بدمج خوارزميتي AES وRSA على التسلسل، وذلك من خلال تطبيق خوارزمية AES لتشفير البيانات في المستوى الأول، ثم تطبيق خوارزمية RSA لتشفير البيانات في المستوى الثاني، ثم تخزينها. وللحصول عليها من قبل المستخدم يقوم بتطبيق خوارزمية RSA لفك تشفير المستوى الثاني، ثم خوارزمية AESلفك تشفير المستوى الأول، ومن ثَمَّ فإن استخدام أكثر من خوارزمية على التسلسل أو التوازي يعطي سرية أكبر لتخزين البيانات لمنع المستخدمين غير الموثوق بهم من الوصول إلى البيانات المخزنة. كما اقترحوا في [13] زيادة سرية البيانات من خلال التشفير متعدد المستويات، وذلك من خلال تشفير الرسالة باستخدام خوارزمية DES كمستوى أول، ثم تشفير النص المشفر الناتج بخوارزمية RSA كمستوى ثانٍ للتشفير على التسلسل، وتخزن الرسالة المشفرة الناتجة، ثم يقوم المستقبل بفك شيفرة الرسالة بخوارزمية RSA، ثم خوارزمية DES على التسلسل للحصول على الرسالة الأصلية، ووجدوا أنَّ استخدام أكثر من مستوى للتشفير يعطي سرية أكبر من مستوى واحد فقط. ودرس الباحثون في [14] الأمن الذي تقدمه خوارزميات RSA وDES (Data Encryption Standard) وAES و(Triple DES) 3DES ووجدوا ان خوارزمية AES هي االفُضْلَى وأنها قابلة للتطوير، إذا ما دُمِجَتْ مع خوارزميات أخرى ومحاولة تطبيق ذلك تسلسلياً أو على التوازي لمعرفة الأفضل بين الطريقتين في الحصول على نظام أمني متكامل. أمَّا البحث [15] فاقترح نموذجاً هجينياً لتأمين سرية البيانات وذلك بدمج AES وDES بتقسيم كل bit 128 من النص إلى قسمين متساويين، وتشفير كل bit 64 بخوارزمية DES على التفرع، ثم تشفير الناتج الـ bit 128 بخوارزمية AES وتطبيق العكس عند فك التشفير، ووجد الباحثون أنَّ النموذج الهجيني أفضل مقاومة للهجمات الجبرية والخطية ويحقق سرية للبيانات أعلى من استخدام كل خوارزمية بمفردها. أمّا في [16] فقد اقترح الباحثون خوارزمية تشفير هجينة بدمج AES وBlowfish وTwofish على التوازي، وذلك لتأمين سرية البيانات. إنَّ الزمن اللازم لإجراء عملية تشفير باستخدام أكثر من خوارزميتين دفع بعض الباحثين لاقتراح أنظمة حماية عدّة تعتمد على خوارزميتين فقط سواء كانت هذه الأنظمة على التسلسل أو على التفرع، إذْ نجد في [17] أنَّ الباحثون طَبَّقُوا خوارزميات

RSA و DES Tripl و Krishna لحماية البيانات من خلال اقتراح عدة أنظمة حماية منها تسلسلية وبعضها تفرعية، إلَّا أنَّ هذه الأنظمة جميعها استخدمت خوارزميتي تشفير فقط سواء كانت تسلسلية أو تفرعية، إذْ لا يوجد في الفرع الواحد إلّا خوارزميتان ورغم هذا الإجراء كانت أزمنة التشفير وفك التشفير كبيرة نسبياً. وأُجري مؤخراً بحث [18] استخدم أكثر من خوارزميتين لاقتراح نظام تشفير وحماية البيانات، اعتمد الباحثون فيه على تقسيم النص إلى ثلاثة أقسام فقط، واكتفوا بتطبيق ثلاث خوارزميات متناظرة فقط، تُطَبَّقُ خوارزمية واحدة على كل قسم من الأقسام الثلاثة للنص ودمجوا بين الخوارزميات الثلاث AES و3DES و RC6 (Rivest Cipher 6) على التوازي، واقترحوا مستقبلياً لزيادة السرية والتصدي للمهاجمين إضافة الخوارزمية غير المتناظرة RSA أيضاً.

4-خوارزمية تشفير RSA [7,6,5] :

تعدّ خوارزمية RSA من أهم خوارزميات التشفير غير المتناظر التي طُوِّرَتْ بواسطة العلماء الثلاثة "Ron Rivest" و "Adi Shamir"و"Leonard Adleman"، تتألف خوارزمية التشفير غير المتناظر RSA من ثلاث مراحل رئيسة:

1-مرحلة توليد المفاتيح.

2-مرحلة التشفير.

3-مرحلة فك التشفير.

يتم توليد المفتاح العام (Public key) PU ليستخدم لتشفير الرسالة قبل إرسالها والمفتاح الخاص (Private key) PR لفك شيفرة الرسالة عند المستقبل؛ وذلك وفق الخطوات:

1: توليد عددين أوليين كبيرين عشوائياً p،q.

2: حساب الجزء المشترك بين المفتاح العام والخاص وفق المعادلة الآتية:

$$n=p.q \qquad (1)$$

3: حساب العامل Ø وفق المعادلة:

$$Ø\,(n)=(p-1)\,(q-1) \qquad (2)$$

4: اختيار عدد صحيح عشوائياً e، عن طريق المعادلة التالية:

$$1<e<Ø\,(n) \qquad (3)$$

$$\gcd(e, Ø\,(n))=1 \qquad (4)$$

إذْ gcd هو القاسم المشترك الأكبر Greatest Common Divisor

5: باستخدام خوارزمية اقليدس الموسعة نحسب العدد الصحيح المميز d:

$$d=e-1(\text{mod } Ø\,(n)) \qquad (5)$$

إذْ mod هو عملية باقي القسمة.

6: يستخدم المفتاح العام PU=(e,n) لتشفير النص عن طريق المعادلة الآتية:

$$C=\ Me\ (\text{mod}\ n) \qquad (6)$$

7: يستخدم المفتاح الخاص PR=(d,n) لفك التشفير عن طريق المعادلة الآتية:

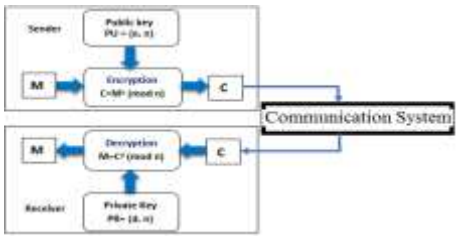
$$M=Cd\ (\text{mod}\ n) \qquad (7)$$

إذْ أنَّ e: أس التشفير (Encryption Exponent)،

d: أس فك التشفير

(Decryption Exponent)، في حين n: يطلق عليها المعامل (Modulus).

يبيّن الشكل (1) المخطط الصندوقي المطبق من أجل تأمين عملية النقل أو التخزين.



الشكل (1) المخطط الصندوقي لعملية نقل البيانات باستخدام خوارزمية RSA [اعداد الباحثين]

7-خوارزميـــة تشـــفير المعيـــار المتقـــدم AES [8,4,3,2]:

تعدّ خوارزمية معيار التشفير المتقدم AES من أهم خوارزميات التشفير المتناظر، وتستخدم تشفير الكتلة، إذْ يُقَسَّمُ النص المراد تشفيره إلى مجموعة من الكتل طول كل كتلة 128خانة، ويجري التشفير باستخدام مفتاح طوله 128 خانة، مدخلات هذه الخوارزمية هي النص الصريح المراد تشفيره ويحول إلى مصفوفة مربعة 4X4 ترمز بـ State ،والمدخل الثاني مفتاح التشفير ويحول إلى مصفوفة مربعة 4X4 ترمز بـCipher Key كما في الشكل الآتي:

State

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

Cipher Key

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

الشكل (2) مدخلات خوارزمية AESمفتاح التشفير والنص الصريح[19]

تتألف من:

1-مرحلة توليد المفتاح وتوسيعه.

2-مرحلة التشفير.

3-مرحلة فك التشفير.

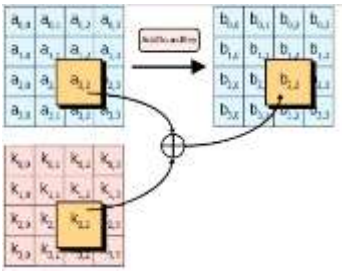
1- مرحلـــــة توليـــــد المفتـــــاح وتوســـــيعه KeyExpansion:

لإنشاء مفاتيح الدورات، يستخدم المعيار AES عملية النشر لمفتاح التشفير الرئيسي. إذا كان عدد الدورات مساويًا لـ N r دورة، فإنّه يجب إنشاء N r + 1 مفتاح دورة بطول 128خانة (Add Round Key). تأخذ خوارزمية AES-128bit مفتاح التشفير كمصفوفة مربعة، كما هو موضّح بالشكل (3) وتقوم بإنجاز تابع توسعة لتوليد مفاتيح مرحلية .

لتنتج مصفوفة خطية من 44 كلمة (11مفتاح)، أي مفتاح الدورة الابتدائية فضلاً عن عشرة مفاتيح، مفتاح لكل دورة.

الشكل (3): كيفية بناء 44 كلمة من أجل خوارزمية AES-128 من المفتاح الأصلي[19]

2- مرحلـــة التشـــفير Encryption: تتـألف عمليـة التشفير من أربع عمليات تحويل عُرِّفَتْ لمعالجة مصفوفة الحالة التي تمثل الشعاع الابتدائي وهي1:- Add Round Key: إضافة مفتاح التشفير إلى النص المدخل باستخدام XORعلى عناصر مصفوفتي الـ Stateوالـ Cipher Key كما في الشكل (4)

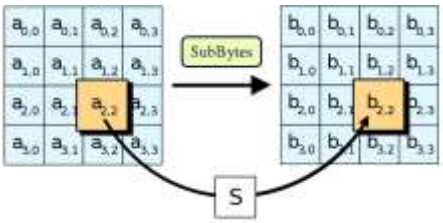


الشكل (4) عملية إضافة مفتاح التشفير Add Round Key[19]

2-Sub Bytes: استبدال بايتات المصفوفة State الناتجة من الدورة الابتدائية السابقة، وذلك من الجدول الجاهز S-box وفق الشكل (5) كما يوضّح الشكل (6) جدول S-box وهو جدول يمثل بمصفوفة مربعة 16×16:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

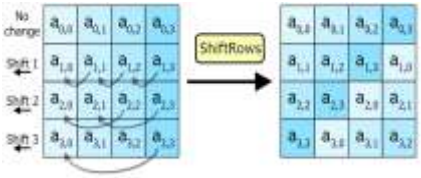
الشكل (5) جدول S-box



الشكل (6) استبدال البايتات Sub Bytes[19]

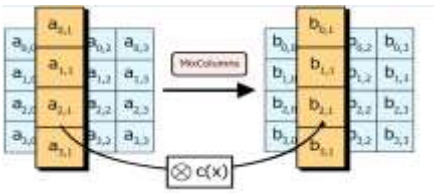
3- Shift Rows: يبيّن الشكل (7) إزاحة سطرية لعناصر أسطر المصفوفة State الناتجة، وفيها يتم تدوير كل سطر من مصفوفة الحالة إلى اليمين كما يأتي: السطر الأول: يتم تدويره بمقدار صفر بايت

(لا يتم تدويره). السطر الثاني: بمقدار بايت واحد. السطر الثالث: بمقدار بايتين. السطر الرابع: بمقدار ثلاثة بايتات.



الشكل (7): إزاحة سطرية Shift Rows[19]

4-مزج الأعمدة Mix columns: ويتم فيها ضرب كل عمود من المصفوفة stateالناتجة بمصفوفة مربعة محددة مسبقاً كما في الشكل (8). وهي العملية الأصعب، إذْ يُعالَجُ كل عمود من مصفوفة الحالة بشكل منفصل للحصول على عمود جديد الذي يُوضَعُ مكان العمود القديم، إو تتضمن العملية جداء مصفوفات وتأخذ عملية Mix columns كل عمود من مصفوفة الحالة و تستبدل به عموداً جديداً يُحْسَبُ بعملية الجداء المصفوفي، إذْ إنَّ العمليات الحسابية المستخدمة تستخدم الحقول المنتهية وليست عمليات حسابية عادية، وهذه الحقول المنتهية لها قواعد خاصة، وعمليات الجداء والجمع يتم تحقيقها باستخدام عملية XOR.



الشكل (8) مزج الأعمدة[19]

3- **مرحلة فك التشفير Decryption:** يمكن فك تشفير للرسالة بخوارزمية AES باستخدام مفتاح التشفير نفسه وعكس تنفيذ مراحل تشفير الرسالة ذلك بحيث يُنَفَّذُ الدوال Inv Mix Columns وInv Shift Rows و Inv Sub Bytes ثمAdd round Key.

1-عكس الدالة Mix Columns: تعمل على مصفوفة state (column-by-column) لتعيد عكس التعبير عن كل بايت بعكس المعادلة.

2-عكسShift Rows: إزاحة للصفوف الثلاثة الأخيرة من المصفوفة State بحيث تعكس الإزاحة عند التشفير.

3-عكس Sub Byte: يجري تبديل باستخدام الجدول العكسي ل S-Box لكل بايت في مصفوفة State

4-Add Round Key: لا تحتاج لعكس لأنَّها في الأصل عملية XOR مع المفتاح، وعلى كل خوارزمية فك التشفير ليست مماثلة لخوارزمية التشفير. ويوضّح الشكل (9) المخطط الصندوقي لعملية التشفير وفك التشفير في خوارزمية AES-128bit لتأمين نقل البيانات وتخزينها[19].

8-ألية الدمج المقترحة لخوارزميتي RSA مع AES:

إن آلية الدمج المقترحة عبارة عن دمج تفرعي لكل من خوارزميتيRSA وAES بغية زيادة السرية مع الحفاظ على زمن تشفير وفك تشفير مناسب، إذْ يتم الإفادة من سرعة خوارزمية AES وخواص الحماية وقوة سريتها مع خواص الحماية والسرية التي تمتع بها خوارزمية RSA مع

محاولة إنقاص الزمن الكبير نسبياً لخوارزمية RSA في مرحلتي التشفير وفك التشفير، تتكون الخوارزمية المقترحة من ثلاث مراحل:1-مرحلة توليد المفاتيح.2-مرحلة التشفير.3-مرحلة فك التشفير.

مرحلة توليد المفاتيح تتم بشكل اعتيادي لكل من خوارزميتي RSA وAES ،إذْ يتولد لدينا ثلاثة مفاتيح:

1-المفتاح السري لـAES.

2-المفتاح العام لـRSA.

3-لمفتاح الخاص لـRSA. لذلك يمكن عَدَّ الخوارزمية المقترحة تتكون من مرحلتين أساسيتين: التشفير وفك التشفير.

8-1-التشفير باستخدام خوارزمية الدمج المقترحة:

يبيّن الشكل (10) خوارزمية الدمج المقترحة لكل من خوارزميتي RSA وAES. إذْ تكون المدخلات:

M: الرسالة المطلوب حمايتها (النص الصريح)، PU=(e,n): المفتاح العام لخوارزمية RSA. PR= (d, n): المفتاح الخاص لخوارزمية RSA، W: المفتاح السري لـ AES

في البداية تجري عملية تجزئة الرسالة M إلى كتل جزئية عددها N تتناسب مع طول النص، كل كتلة بطول 128bit، بعد إجراء عملية التقسيم إلى كتل جزئية عددها N تُوَزَّعُ الكتل على التوالي لخوارزميتي AES وRSA ضمن حلقة تكرارية بفرعين: فرع لـ AES وفرع لـ RSA من خلال متحول (L) الذي يقوم بالتحكم بعملية توزيع الكتل وفق المعادلة الشرطية:

$$C_i = \begin{cases} RSAe(m_i); & L = 0 \\ AESd(m_i); & L = 1 \end{cases} \qquad (8)$$

إذْ m_i: الكتلة الجزئية ذات الترتيب i.

RSA: إجراء فرعي يقوم بالتشفير باستخدام خوارزمية RSA وفق المعادلة (6).

AES: إجراء فرعي يقوم بالتشفير باستخدام خوارزمية AESالموضّح في الفقرة (6)

Ci: النص المشفر ذو الترتيب i.

بعد انتهاء حلقة التشفير تبدأ عملية تجميع الكتل المشفرة Ci لنحصل في النهاية على النص المشفر C.

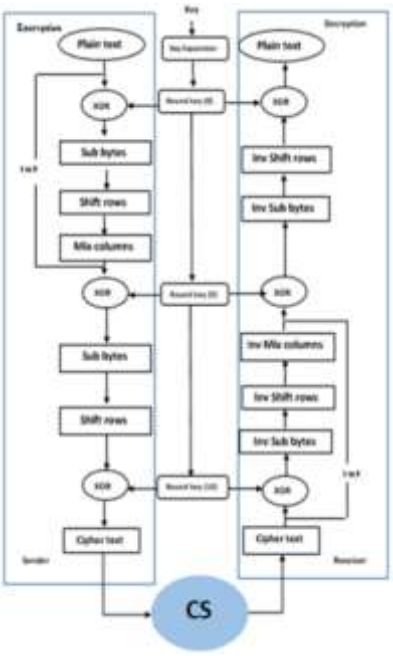
8-2-فك التشفير باستخدام خوارزمية الدمج المقترحة:

يبيّن الشكل (11) كيفية إجراء عملية فك التشفير باستخدام آلية الدمج المقترحة لكل من خوارزميتي RSA وAES. إذْ يكون دخل الخوارزمية النص المشفر C ثم تأتي مرحلة تجزئة هذا النص إلى كتل فرعية Ci بعدها تبدأ حلقة فك التشفير مكونة من فرعين على التوازي: فرع فك التشفير باستخدام RSA وفق المعادلة (7)، وآخر باستخدام AES كما هو مبيّن بالفقرة (6)، وفي النهاية تجري عملية تجميع الكتل mi الناتجة عن فك التشفير لنحصل على النص الصريح M.

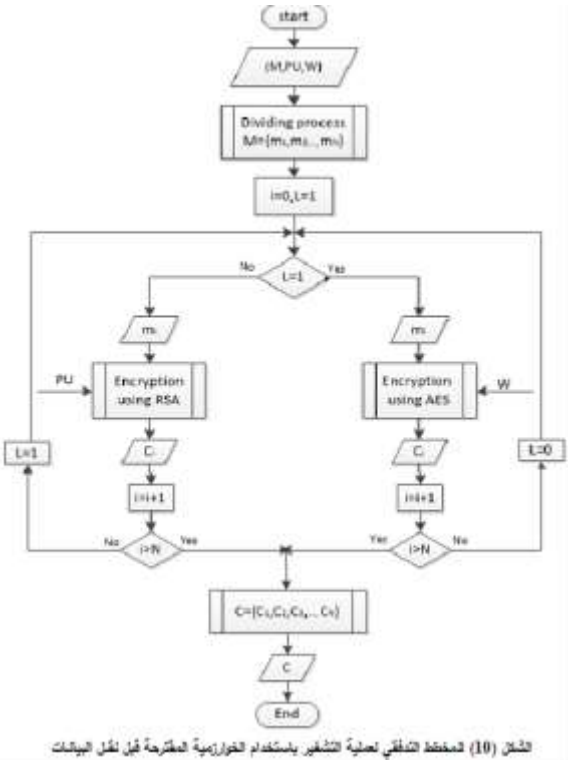
9-النتائج والمناقشة:

صُمِّمَ نظام برمجي لحماية البيانات يعتمد على خوارزميتي RSA وAES إذْ يمكن من خلال هذا النظام إجراء عملية التشفير إمّا بخوارزمية RSA أو AES، أو خوارزمية الدمج المقترحة، كما هو مبيّن بالشكل(12). يتكوَّن النظام من قسمين رئيسيين قسم التشفير، وقسم فك التشفير. ويتيح النظام خيارات للتشفير إذْ يمكن إجراء التشفير وفك التشفير باستخدام خوارزمية RSA كما في الشكل (12).

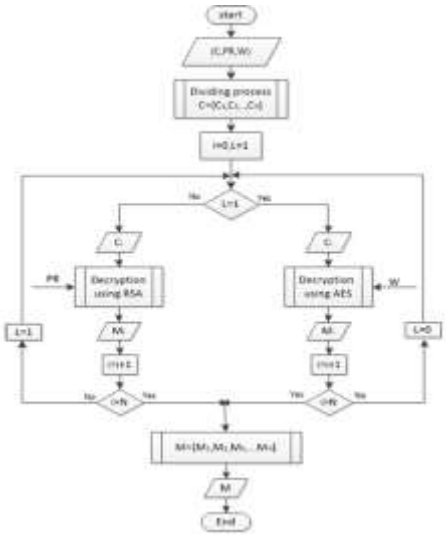
تمت عملية برمجة خوارزمية RSA الموضّحة في الفقرة (5)، في حين تمت عملية برمجة خوارزمية AES الموضّحة بالفقرة(6)، ويمكن إجراء عملية حماية البيانات من خلال تشفيرها باستخدام خوارزمية AES ثم فك تشفيرها بالخوارزمية نفسها، وهو أيضاً خيار يتيحه لنا النظام المبرمج في البيئة البرمجية Matalab . الخيار الثالث والأخير لحماية البيانات هو حمايتها باستخدام خوارزمية الدمج المقترحة التي وُضِّحَتْ في الفقرة (8) التي تعتمد على دمج خوارزميتي RSA وAES على التوازي. لمعرفة مدى فعالية خوارزمية الدمج المقترحة أُجْرِيَتْ عملية مقارنة لأزمنة التشفير وفك التشفير لملفات عدّة بأحجام مختلفة، وقُورِنَتْ هذه الأزمنة بأزمنة خوارزميتي RSA وAES.



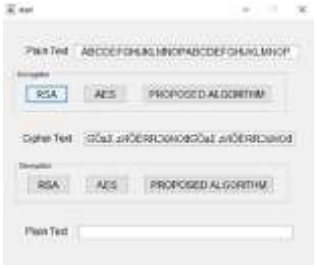
الشكل (9) المخطط الصندوقي لعملية التشفير وفك التشفير باستخدام خوارزمية AES



الشكل (10) المخطط التدفقي لعملية التشفير باستخدام الخوارزمية المقترحة لكل البيانات



الشكل (11) المخطط التدفقي لعملية فك التشفير بعد نقل البيانات باستخدام الخوارزمية المقترحة.



الشكل (12) نظام حماية البيانات وفق الخوارزميات RSA وAES وخوارزمية الدمج المقترحة

يبـيّن الجـدول (2) أحجـام الملفـات التـي تـم حمايتهـا والأزمنـة اللازمـة (التـي حُسِبَتْ باستخدام برنامج matlab) لتشفيرها وفق الخوارزميات الثلاث RSA وaes وخوارزمية الدمج المقترحة.

الجدول(2) زمن التشفير للنص المرسل لكل من خوارزمية RSA وAES وخوارزمية الدمج.

حجم الملف	خوارزمية RSA	خوارزمية AES	خوارزمية الدمج المقترحة
50KB	552ms	123ms	338.5
100KB	1112ms	239ms	676.5
150KB	1630ms	306ms	969
200KB	2063ms	499ms	1282

في حين يبيّن الشكل (13) المنحنيات البيانية الناتجة عن هذه الأزمنة، إذْ يبيّن أنَّ الخوارزمية المقترحة تحتاج إلى زمن أقل من الزمن الذي تحتاجه RSA لإجراء عملية التشفير إلَّا أنَّها – خوارزمية الدمج المقترحة– تحتاج لزمن أعلى من الزمن الذي تحتاجه خوارزمية AES الأساسية، لكنها تؤمن حماية أعلى من كلتا الخوارزميتين RSA وAES كما هو مبيّن بالجدول (3) إذْ نجد أنَّ هذه الخوارزمية أعطت أعلى معدل أنتروبي للبايت الواحد Average entropy per byte، وذلك لأنَّها تعطي نصاً مشفراً هو خليط من تشفير الخوارزميتين السابقتين، الأمر الذي يضيف عقبات أكثر أمام المخترق للحصول على النص الأصلي. وقد حُسِبَتْ وفق العلاقة الآتية[20]:

$$Entropy = \sum_{i=1}^{2N} P(B_i)\log\left(\frac{1}{P(B_i)}\right) \qquad (9)$$

إذْ: $P(B_i)$ احتمالية ورود البايت B_i في النص، N حجم النص بالبايت، ويبيّن الجدول (4) أزمنة فك التشفير لخوارزمية RSA وAES وخوارزمية الدمج المقترحة التي حُسِبَتْ باستخدام برنامج matlab.

الجدول (3) قيم معدل الانتروبي لكل من خوارزمية RSA وAES والمقترحة

الخوارزمية	خوارزمية RSA	خوارزمية AES	خوارزمية الدمج المقترحة
معدل الإنتروبي للبايت الواحد	3.1	3.85	5.95

الجدول (4) زمن فك التشفير للنص المرسل لكل من خوارزمية RSA وAES والمقترحة

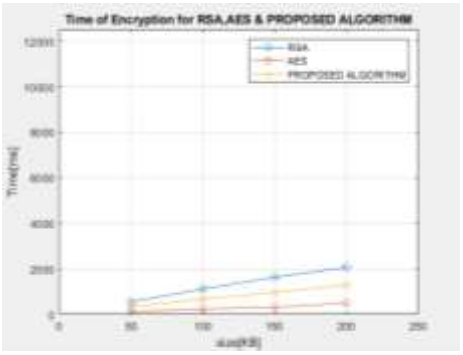
حجم الملف	خوارزمية RSA	خوارزمية AES	خوارزمية الدمج المقترحة
50KB	2103ms	470ms	1288
100KB	4025ms	910ms	2469
150KB	6440ms	1220ms	3831
200KB	8200ms	1760ms	4981

كما يبيّن الشكل (14) المنحنيات البيانية لهذه الأزمنة، إذْ نلاحظ أنَّ خوارزمية الدمج المقترحة تحتاج لزمن أكثر من AES لكنه أقل من RSA.

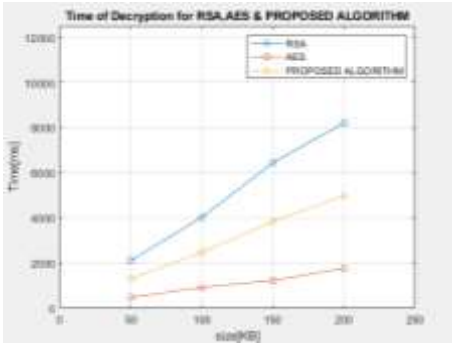
قُورِنَتْ أزمنة التشفير وفك التشفير للخوارزمية المقترحة بالنتائج الواردة في المرجع [21]، إذْ اقترح الباحث خوارزمية دمج لتشفير الصور؛ وذلك من خلال حساب متوسط زمن تشفير البايت الواحد ومتوسط زمن فك التشفير له، كما هو مبيّن بالجدول (5)، كما قُورِنَ ببحث قام بدمج خوارزميتي RSA وAES لكن نجد أنَّ الطريقة المقترحة في هذا البحث أعطت زمن تشفير وزمن فك تشفر أقلّ من الطريقة المتبعة في البحث [22]، وذلك لأنَّ الباحثين دمجوا خوارزميتي RSA تسلسلياً، ممّا أضاف زمناً أطول لتنفيذ خوارزميتي RSA وAES، وهذا ما يفسر تفوق الخوارزمية المقترحة في هذا البحث على طرائق الدمج المتبعة في البحوث المبين نتائجها في الجدول (5). ويرجع اختلاف الأزمنة بين البحوث إلى اختلاف التجهيزات الصلبة من ناحية المواصفات كسرعة المعالج وغيرها، ويرجع سبب الزمن الكبير الموجود في الدراسة [24] لدمج ثلاث خوارزميات.

الجدول (5) مقارنة بين الخوارزمية المقترحة في هذا البحث بخوارزميات مقترحة في دراسات مرجعية

الخوارزمية	متوسط زمن تشفير البايت الواحد	متوسط زمن فك تشفير البايت الواحد	معدل الأنتروبي
الخوارزمية المقترحة	1ms	2.5ms	5.95
المقترحة في [21]	3.25ms	3.5ms	3.59
خوارزمية دمج RSA+AES[22]	4ms	7ms	لم يذكر
خوارزمية دمج RSA+AES[23]	1.2378ms	2.647ms	لم يذكر
خوارزمية دمج RSA+AES+Twofish[24]	4.71ms	3.97ms	لم يذكر



الشكل (13) زمن التشفير لخوارزمية الدمج المقترحة وكل من خوارزميتي RSA وAES.



الشكل (14) زمن فك التشفير لخوارزمية الدمج المقترحة وكل من خوارزميتي RSA وAES

10-الخاتمة:

في هذا البحث صُمِّمَ نظام لحماية البيانات في أثناء إرسالها وتخزينها ضمن الشبكة، ويتيح هذا النظام إمكانية الحماية وفق خوارزمية RSA وAES و خوارزمية الدمج المقترحة، اِعْتُمِدَ في هذا البحث على تقسيم الملف إلى كتل جزئية، كل كتلة بطول 128bit لتحقيق التلاؤم ما بين خوارزميتي RSA وAES، وحققت هذه الخوارزمية زمن تشفير وفك تشفير أقل من خوارزمية RSA، ومن ثَمَّ تعدّ أسرع منها إلّا أنَّها أبطأ من خوارزمية AES، لكنها أضافت سرية أعلى من أجل حماية البيانات إذْ أعطت أعلى معدل أنتروبي للبايت الواحد من خلال إضافة عقبات أكثر إلى المهاجم، وهي عدم معرفة الكتل المشفرة بأي خوارزمية تم تشفيرها RSA أو AES، ووجود مفتاح جلسة سري فضلاً عن مفتاح خاص؛ ممّا يؤمن خصوصية كل مستخدم، فضلاً عن وجود ميزات الحماية التي تمتع بها كل من خوارزميتي RSA وAES.

References المراجع

[1]Hilal Nur Issı, Ahmet Efe," CRYPTOGRAPHY CHALLENGES OF CLOUD COMPUTING FOR E-GOVERNMENT SERVICES" International Journal of Innovative Engineering Applications 2, 1 (2018), 4-14.

[2]Abha Sachdev, Mohit Bhansali,"Enhancing Cloud Computing Security using AES Algorithm" International Journal of Computer Applications (0975–8887) Volume 67–No.9, April 2013.

[3]Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi "Data Security in Cloud Computing Using AES Under HEROKU Cloud", 978-1-5386-4959- 6/18/$31.00 ©2018 IEEE.

[4]Tamilselvi.S," Data Storage Security in Cloud Computing Using AES" International Journal of Advanced Networking & Applications (IJANA) Volume: 08, Issue: 05 Pages: 124-127 (2017) Special Issue.

[5]Faraz Fatemi Moghaddam, Maen T. Alrashdan, and Omidreza Karimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments"Journal of Advances in Computer Network, Vol. 1, No. 3, September 2013.

[6]Dr. D.I. George Amalarethinam, H. M. Leena,"Enhanced RSA Algorithm with arying Key Sizes for Data Security in Cloud", 978-1-5090-5573-/16$31.00©2016IEEEDOI10.1109/ WCCCT.2016.50.

[7]SHAMBHAVI1, DR. SONAL SHARMA2, "Enhanced RSA Algorithm for Data Security in Cloud" © MAR 2018 | IRE Journals | Volume 1 Issue 9 | ISSN: 2456- 8880.

[8]Omar G.Abood, Shawkat K.Guirguis "A Survey on Cryptography Algorithms" http://dx.doi.org/10.29322/IJSRP.8.7.2018.p7978.

[9]Gurjeet Singh, Dr. Mohita Garg, "Enhanced Cloud Security using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption with Secure OTP", International Journal of Computers&TechnologyVol18(2018)ISSN:2277-3061 https://cirworld.com/index.php/ijct.

[10]R.Kalaivani, "Triple Layer Security to Data in Cloud" R.Kalaivani / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (2), 2016, 783-785.

[11] Navdeep Singh, Pankaj Deep Kaur,"A Hybrid Approach for Encrypting Data on Cloud to prevent DoS Attacks", International Journal of Database Theory and ApplicationVol.8, No.3 (2015), pp.145-154http://dx.doi.org/10.14257/ijdta.2015.8.3.12.

[12]Rasmi M "Multilevel Security in Cloud Computing", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Published by,www.ijert.org,NSDMCC - 2015 Conference Proceedings.

[13]Shakeeba S. Khan,Prof.R.R.Tuteja,"Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.

[14]V. Vanitha Devi, R. Kalaiselvi, K. Kousalya, "A Survey on Enterprise Software Encryption Algorithms", Conference Proceeding of 2nd International Conference on Engineering Technology, Science and Management Innovation (ICETSMI-2017) at National Institute of Technical Teachers Training & Research (NITTTR),MHRD, Govt of India, Chandigarh, India on 15th January 2017 ISBN: 978-81-932712-3-0

[15]Jignesh R Patel, Rajesh S. Bansode, Vikas Kaul," Hybrid Security Algorithms for Data Transmission using AES-DES", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.2, February 2012 – www.ijais.org.

[16]Neha, Mandeep Kaur,"Enhanced Security using Hybrid Encryption Algorithm", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 7, July 2016.

[17]Ali Abdulridha Taha, Dr. Diaa Salama AbdElminaam, Prof.Dr. Khalid M Hosny,"NHCA: Developing New Hybrid Cryptography Algorithm for Cloud Computing Environment", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.

[18]Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam,"Secure File Storage on Cloud using Hybrid Cryptography",© 2019,

IJCSE All Rights Reserved 587 International Journal of Computer Sciences and Engineering Open Access Review Paper Vol.-7, Issue-1, and Jan 2019 E-ISSN: 2347-2693.

[19]Bloc,"Advanced Encryption Standard", meilleur cryptanalyse,2019.

[20]Shaheen Ayyub, Praveen Kaushik,"Secure Searchable Image Encryption in Cloud Using Hyper Chaos", The International Arab Journal of Information Technology, Vol. 16, No. 2, March 2019

[21] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3

[22] Ritin Behl, Garima Sehgal, Mridula Kumar, Pushkar Gupta, Shubham Garg, "Experimental comparison between Hybrid RSA-AES and RSA algorithms in IP security", IJMTER, Volume 02, Issue 06, [June – 2015] ISSN (Online):2349–9745; ISSN (Print):2393-8161

[23] Shashikant Kuswaha, Praful B.Choudhary, Sachin Waghmare, Nilesh Patil," Data Transmission using AES-RSA Based Hybrid Security Algorithms", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 4, April 2015

[24] Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption", Journal of Information Security, 2018, 9, 168-176.

Received	30/5/2019	إيداع البحث
Accepted for Publ.	6/11/2019	قبول البحث للنشر