Damascus University Journal for the Basic Sciences
Vol 41 No.3 (2025): 25 -43

مجلة جامعة دمشق للعلوم الأساسية
مجلد 41-عدد 3 (2025): 25- 43

دِرَاسَةٌ حَولَ زِيَادَةِ استِيقَانِ الرَّسَائِلِ النَّصِّيَّةِ المُرْسَلَةِ باستِخْدَامِ خَوَارِزْمِيَّاتِ التَّوقِيعِ الرَّقْمِيِّ

ماجد محمد الخيرو
majed.alkhairow@damascusuniversity.edu.sy

المُلخَّصُ

قمنا في هذا البحثِ باقتراح نموذجًا لزيادةِ استيقانِ الرَّسائلِ المُرسلةِ عبرَ الشَّبكةِ. هذا النموذج يمر بمرحلتين على الشكل الآتي: **المرحلـة الأولـى:** تطويرُ خوارزميَّـةِ الـ MD5 التي تُعتبرُ الخوارزميّـةَ الأساسيَّـةَ والشاملـةَ التي انطلـقَ منهـا التَّوقيـعُ الرَّقمـيُّ، حيثُ قمْنـا بالتَّعديلِ على العمليَّاتِ المنطقيَّةِ، وبتغييرِ اتِّجاهِ الإزاحةِ من اليسارِ إلى اليمينِ، وتوصَّلْنا إلى زمنِ تنفيذٍ أقلَّ. **الثَّانية:** دمجُ خوارزميَّتِنا المعدَّلةِ معَ خوارزميَّةِ التَّوقيعِ الرَّقْميّ SHA-1؛ وذلكَ لزيادةِ استيقـانِ الرَّسائلِ المُرسلةِ. أخيرًا قمْنا باختبارِ نموُذَجُنا المقترحِ من خلالِ برمجتِهِ بلغةِ البرمجةِ C#.

الكلماتُ المفتاحيَّةُ: التَّوقيعُ الرَّقْميُّ، استيقان، MD5، SHA-1.

تاريخ الإيداع: 2023/11/26
تاريخ الموافقة: 2024/01/21

ISSN (online): 2789-6366
http://journal.damascusuniversity.edu.sy/index.php/index/index

A Study about Increasing the Authentication of Messages Text Sent using Digital Signature Algorithms

Majed Mohammad Alkheirow
majed.alkhairow@damascusuniversity.edu.sy

Abstract

In this paper, we propose a model to increase the authenticity of messages sent over the network, Our model went through two stages:

The first: the modification of the MD5 algorithm, which is the basic and comprehensive algorithm from which the Digital Signature was launched, Where we have modified the logical operations, by changing the direction of shift from left to right. We came up with a lower execution time.

The Second: the integration of our modified algorithm with Digital Signature algorithms; in order to increase the authenticity of the sent messages.

Received :2023/11/26
Accepted:2024/01/21

Keywords: Digital Signature, Authentication, MD5, SHA-1.

1. المقدمة (Introduction)

يَشهدُ العالَمُ وبشكلٍ كبيرٍ تطوُّرًا هائلًا ومُتسارعًا في مجالِ تكنولوجيا عالَمِ الاتِّصالِ حتَّى أصبحَتْ وسائلُ الاتِّصالِ الحديثةِ وعلى رأسِها الانترنتُ مِن الوسائلِ الَّتي لا يُمكنُ الاستغناءُ عنها. بعدَ أنْ كانَتِ الاتِّصالاتُ تعتمدُ على الهاتفِ ثُمَّ الفاكسِ، ظهرَ الانترنتُ وأصبحَ الوسيلةَ المُثلَى في الاتِّصالِ ونَقْلِ المعلوماتِ وتقديمها. لقد بدَتِ الحاجةُ مُلِحَّةً لِحمايةِ هذهِ المعلوماتِ واستيقانِها وإثباتِ أصالتِها. مِنْ هُنا ظهرَ ما يُسمَّى بالتَّوقيعِ الرَّقْمي. أُستُخدِمَ التَّوقيعُ الرَّقْميُّ لأوَّلِ مرَّةٍ في فرنسا في مجالِ البطاقاتِ الائتمانيَّةِ عامَ 1989م[4]. تعتمدُ فكرةَ خوارزميَّةِ التَّوقيعِ الرقميَّ على استبدالِ التَّوقيعِ اليدويّ بالمكافئِ الرَّقمي، والغرضُ مِن هذهِ الخوارزميَّاتِ تمكينُ المُستخدمِينَ مِن تبادُلِ الرَّسائلِ بالإضافةِ لتأكيدِ هُويَّةِ الشَّخصِ المُرسِلِ للرِّسالةَ. أصبحَتِ القدرةُ على تبادُلِ الرَّسائلِ وإثباتِ أصالتِها محطَّ اهتمامِ الباحثِينَ، إذْ بدأَتْ قدرةُ الخَوارزميَّاتِ تَضعُفُ مَعَ مرورِ الزَّمنِ، وهذا ما دفعَنا إلى تعزيزِ قُدرةِ الخوارزميَّاتِ مِنْ خِلالِ عمليَّاتِ التَّهجينِ.

في هذا البحثِ قُمْنا بدايةً بتعديلِ خوارزميَّةِ MD5 الأصليَّةِ، بالإضافةِ لذلكَ عزَّزْنا عمليَّةَ التَّوقيعِ الرَّقْميّ باقتراحِ نموذجٍ يَضمَنُ عدَمَ العبَثِ بالرَّسائلِ المُرسَلةِ، حيثُ يعتمدُ نموذجُنا على التَّشفيرِ في خوارزميَّتِنا المُعدَّلةِ مرَّةً والتَّشفيرِ في خوارزميَّة SHA – 1 مرَّةً أخرى، والحصولِ على بصمتَينِ ناتجتَينِ، ثُمَّ دَمْجِ تلك البصمتَينِ النَّاتجتَينِ والحصولِ على بصمةٍ مُدمَجةٍ. بعدَ ذلكَ سنقومُ بإرسالِ الرِّسالةِ والبصمةِ المُدمجةِ إلى المستقبلِ الَّذي بدورِهِ سيقومُ بتشفيرِ الرِّسالةِ باستخدامِ خوارزميَّتِنا المُعدَّلةِ (MMD5) مرَّةً والتَّشفيرِ في خوارزميَّةِ SHA – 1 مرَّةً أخرى، والحصولِ على بصمتَينِ ناتجتَينِ، ثُمَّ يقومُ بفكِّ دَمْجِ البصمتَينِ والحصولِ على البصمتَينِ الأساسيَّتَينِ التَّابعَتَينِ لعمليَّةِ الدَّمْجِ. أخيرًا يتُمُّ إجراءُ مقارنةٍ بينَ بصمتَي MMD5 النَّاتجتَينِ عن تشفيرِ المُستقبِلِ وفكِّ الدَّمْجِ، ومقارنةِ بصمتَي SHA-1 النَّاتجتَينِ عن تشفيرِ المُستقبِلِ وفَكِّ الدَّمْجِ، وهُنا نُميِّزُ حالتَينِ:

<u>الحالةُ الأولى</u>: إذا كانَتِ بصمتَا المُستقبِلِ والمُرسِلِ لِخوارزميَّةِ الـ MMD5 متطابقتَينِ، وبصمتَا المُستقبِلِ والمُرسِلِ لخوارزميَّةِ الـ SHA-1 متطابقتَينِ، تظهرُ عندَئذٍ الرِّسالةُ الأصليَّةُ.

<u>الحالةُ الثَّانيةُ</u>: إذا كانَتِ بصمتَا المُستقبِلِ والمُرسِلِ لخوارزميَّةِ الـ MMD5 مختلفتَينِ أو بصمتَا المُستقبِلِ والمُرسِلِ لخوارزميَّةِ الـ SHA-1 مختلفتَين، يتمُّ عندئذٍ تنبيهُ المستخدمِ بذلكَ و إظهارُ الكلمةِ "Error".

قدَّمْنا في هذا البحثِ توضيحًا لأساسيَّاتِ ومفاهيمِ خوارزميَّاتِ التَّوقيعِ الرَّقْميّ.

2. فكرةُ البحثِ وأهدافُهُ (Idea and objectives)

رَغمَ وُجودِ العديدِ مِن الدِّراساتِ المُتعلِّقةِ بأمْنِ المَعلوماتِ بشكلٍ عامٍ وبخوارزميَّاتِ التَّوقيعِ الرَّقْمِيّ بشكلٍ خاصّ، إلَّا أنَّهُ لم تُقدِّمْ حلولًا شاملةً لكافَّةِ المشاكلِ، فعلى سبيلِ المثالِ: وجودُ طَرَفٍ ثالثٍ بينَ طرفَي الاتِّصالِ وانتحالِهِ لشخصيَّةِ أحدِ الطرفَينِ. **بعبارةٍ أخرى تكمُنُ المُشكلةُ في التَّساؤُلاتِ الَّتي سَنقُومُ بعرضِها:**

1. هل يُمكِنُ تقليلُ زمَنِ تنفيذِ خوارزميَّةِ MD5 باعتبارِها الأكثرَ شيوعاً؟
2. هل يُمكنُ كشفُ عمليَّةِ الانتِحالِ عندَ وجودِ سيناريو انتِحالِ شخصيَّةِ أحَدِ طرفَي الاتِّصالِ؟
3. هل يُمكنُ تعزيزُ وثوقيةِ الرَّسائلِ المُتبادَلةِ بينَ طرفَي الاتِّصالِ؟ وهل يُمكنُ الاستِفادةُ مِن الخوارزميَّاتِ الموجودةِ لِتحقيقِ ذلك؟

نُقدِّمُ في هذا البحث نموذجًا مُطوَّرًا لِدَمْجِ خوارزميَّاتِ التَّوقيعِ الرَّقْميّ؛ مِمَّا يُؤدِّي إلى زيادةِ الاستيقانِ للرَّسائِلِ المُشفَّرةِ، ومِنْ أجلِ تحقيقِ ذلكَ ضِمْنَ زمَنٍ مقبولٍ قُمْنا بإجراءِ تعديلٍ على خوارزميَّةِ MD5 للحُصُولِ على زَمَنِ تنفيذٍ أقَلَّ.

3. مَوادُّ البحثِ وطرقُهُ (Materials and Methods)

3-1 المفاهيمُ الأساسيَّةُ في التَّوقيعِ الرَّقْميّ (Basic concepts in Digital Signature)

3-1-1 النَّصُّ الصَّريحُ (Plain Text)

النَّصُّ الصَّريحُ هُوَ عبارةٌ عَن الرِّسالةِ الأصليَّةِ أو المعطياتِ الَّتي تشكِّلُ مَدخلَ عمليَّةِ التَّشفيرِ [1].

3-1-2 الاستيقانُ (Authentication)

عندَ النَّظرِ إلى مفهومِ الاستيقانِ (الصِّحَّة)، فلا بُدَّ من التَّمييزِ بينَ استيقانِ شريكِ الاتِّصالِ واستيقانِ البياناتِ[7][8]، وسنُوضِّحُ كِلَيهِمَا كَمَا يأتي:

I. **استِيقانُ شريكِ الاتِّصالِ:** هذا يعني أنَّ الطرفَ الثاني هو الشَّخصُ الَّذي يَدَّعِي أنَّه هُوَ شَّريكَ الاتِّصالِ، وبالتالي فهو لا يملكُ القدرةِ على إنكارِ إرسالِ أو استقبالِ رسالةٍ ما. يُمكنُ تقسيمُ عدمِ الإنكارِ إلى نوعَينِ. **النوع الأوَّل** هو عدمُ إنكارِ المصدرِ، وهذا يعني أنَّ المُرسِلَ لا يُمكِنُهُ الإنكارُ بأنَّهُ هو مصدرُ البياناتِ. أما **النوع الثَّاني** فهُو عدمُ إنكارِ الاستلامِ، أي أنَّ شريكَ الاتِّصالِ لا يُمكنُه إنكارُ أنَّهُ استلمَ البياناتِ.

II. **استِيقانُ البياناتِ:** تعني أنَّ البياناتِ تمَّ توليدُها مِن طرفِ الاتِّصالِ المفترَضِ.

3-1-3 السِّرِّيَّةُ (Confidentiality)

السِّرِّيَّة هيَ ضَمانُ إمكانيَّةِ الوصولِ إلى الرِّسالةِ مِن قِبَلِ الأشخاصِ المعنيّينَ فَقَطْ [7].

3-1-4 التَّكامُلُ (Integrity)

التَّكامُلُ يعني أنَّ إمكانيَّةَ التَّعديلِ تكونُ مُمكنةً فَقَطْ للأشخاصِ المُصرَّحِ لَهُم بذلكَ [7].

3-1-5 عَدَمُ الإنكارِ (Non-repudiation)

عَدَمُ الإنكارِ هوَ ضمانُ أنَّهُ لا يُمكنُ للمُرسِلِ إنكارُ إرسالِ الرَّسائلِ ولا يُمكنُ للمُستقبِلِ إنكارُ استقبالِ الرَّسائلِ[8].

3-1-6 التَّحكُّمُ في الوصولِ (Access Control)

التَّحكُّمُ في الوصولِ هو تحديدِ مُستَوى الوصولِ المسموحِ بهِ مِنَ المعلوماتِ لكلِّ شخصٍ[8].

3-1-7 الإتاحِيَّةُ (Availability)

الإتاحِيَّةُ هِيَ التَّأكُّدُ مِنَ استمرارِ العَمَلِ والقدرةِ على تقديمِ الخِدمةِ المَطلوبةِ وضَمانِ إمكانيَّةِ الأشخاصِ المُخوَّلِ لهم الوصولُ إلى المعلوماتِ[6].

3-1-8 الهَجمَاتُ (Attacks)

الهُجومُ هُوَ اعتداءٌ يهدفُ إلى اختراقِ السِّياسةِ الأمنيَّةِ والحصولِ على هدفٍ مُحدَّدٍ، وبناءً على تلك الأهدافِ تُقسَمُ الهجماتُ لعدَّةِ أنواعٍ، وهِيَ: هجومُ تحليلِ التَّردُّدِ، وهجومُ تعديلِ المُحتَوى، وهجومُ التَّزويرِ، وهجومُ المُقابلةِ في المُنتصَفِ[6].

I. هُجُومُ تحليلِ التَّردُّدِ (Frequency Analysis Attack)

مِنَ المعلومِ أنَّ لكلِّ لُغةٍ مِن اللُّغاتِ مَيّزاتٍ خاصَّةً بها مِنْ حيثُ التّكرارُ سواءً أكانَ هذا التّكرارُ يتعلّقُ بعددِ الأحرفِ أم بعددِ الكلماتِ الثُّنائيَّةِ أم الثُّلاثِيَّةِ وغيرِها. في هذا النَّوعِ مِن الهُجُومِ يُحلِّلُ المُهاجِمُ الشِّيفرةَ الَّتي وصَلَ إليها، ويُحاوِلُ معرفةَ الأحرفِ أو الكلماتِ الأكثرِ تكرارًا حتَّى يَصِلَ إلى المِفتاحِ الَّذي يَفُكُّ الشّيفرةَ.

II. هُجُومُ تعديلِ المُحتَوَى (Modification Attack)

هُجُومُ تعديلِ المُحتوَى يعني أنْ يقومَ الطَّرفُ غيرُ المُخوَّلِ له باستقبالِ البياناتِ مِنَ المُرسِلِ وتغييرِ محتواها وإعادةِ إرسالِها إلى الطَّرفِ المُستقبلِ.

III. هُجُومُ التَّزويرِ (Fabrication Attack)

هُجُومُ التَّزويرِ يعتمدُ على إرسالِ البياناتِ للمُستقبِلِ مِن خلالِ طرفٍ غيرِ مَعْنيٍّ بحيثُ تبدو وكأنَّها مُرسَلَةٌ مِن طرَفٍ مَعرُوفٍ.

IV. هُجُومُ المُقابلةِ في المنتصَفِ (Man-in-the-Middle Attack)

في هُجُومِ المقابلةِ في المُنتصفِ يقومُ المُهاجِمُ بتحليلِ البَيَاناتِ المُرسَلَةِ والمُستقبِلةِ بينَ طرفَي الاتِّصالِ لكَشْفِ مِفتاحِ التَّشفيرِ.

2-3 بعضُ خوارزميَّاتِ التَّوقيعِ الرَّقميّ [8] [5] [4] [2] [1]

إنَّ خوارزميَّاتِ التَّوقيعِ الرقميّ تُشبهُ خوارزميَّاتِ التَّشفيرِ، لكنَّ الَّذي يُميِّزُها عن خوارزميَّاتِ التَّشفيرِ هُوَ أنَّها خوارزميَّاتٌ ذاتُ اتِّجاهٍ وحيدٍ، وأنَّها تأخُذُ رسائلَ بأطوالٍ مختلفةٍ، كلٌّ مِنها تُخرِجُ بصمةً بطولٍ ثابتٍ، نذكرُ بعضَها: خوارزميَّة (Message Digest 5, MD5)، حيثُ تُعتبَرُ هذهِ الخوارزميَّةُ أوَّلَ ظهورٍ للتَّوقيعِ الرقميّ، وتَمَّ تصنيفُها بخوارزميَّةٍ مِنَ الجِيلِ الأوَّلِ. أمَّا في الجيلِ الثَّاني فقد طُوِّرَتْ خوارزميَّةُ الـ MD5 في عامِ 1995م وسُمِّيَتْ بخوارزميَّةِ الـ SHA – 1 والحصول على بصمةٍ أطول. كَمَا اكتُشِفَ مُؤخَّرًا الجيلُ الثَّالثُ مِنَ الخوارزميَّةِ وسُمِّيَتْ بخوارزميَّةِ الـ SHA – 2، الَّتي بدورِها تنقسمُ إلى عدةِ خوارزمياتٍ فرعيةٍ كما يلي:– SHA و SHA – 256 و SHA – 224) (SHA – 512 و 384 كَمَا في الجدولَ (1). سندرسُ من هذه الخوارزميات خوارزميَّةَ الـ MD5 الَّتي تُعتبَرُ حجرَ الأساسِ لجميعِ خوارزميَّاتِ التَّوقيعِ الرَّقميّ المطوَّرةِ بعدَها.

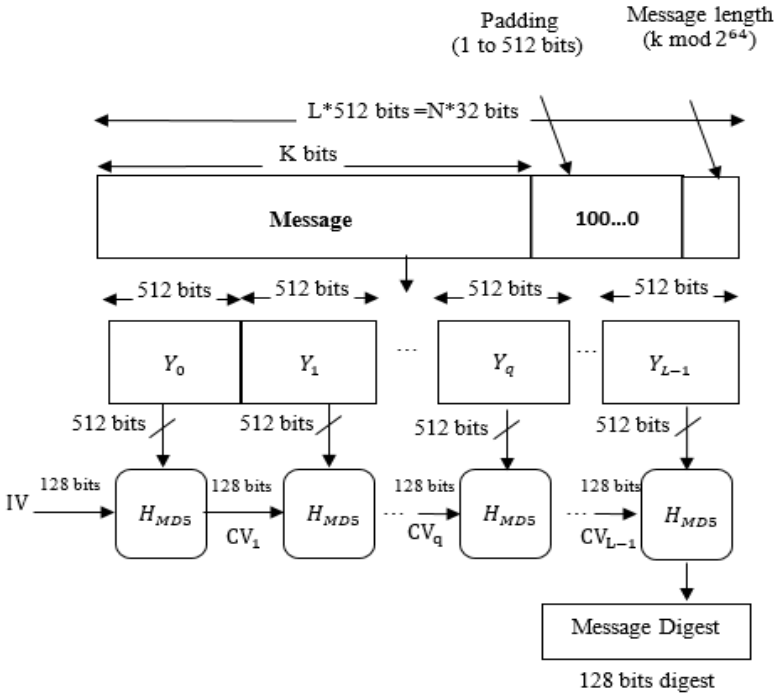
الجدولُ (1): بعضُ خوارزميَّاتِ التَّوقيعِ الرَّقميّ وأطوال البصمةِ لكلِّ خوارزميَّةٍ.

الخَوَارِزْمِيَّةُ	طُولُ البَصْمَةِ
MD5	128 bit
SHA-1	160 bit
SHA-224	224 bit
SHA-256	256 bit
SHA-384	384 bit
SHA-512	512 bit

1-2-3 خوارزميَّةُ (Message Digest 5, MD5)

تأخُذُ خوارزميَّةُ MD5 رسائلَ بأطوالٍ غيرِ محدَّدةٍ، وتُعطِي على الخَرْجِ بصمةً بطولٍ ثابتٍ 128 بتًّا، مِنْ ناحيةِ المدخلاتِ يكونُ طولُ الرِّسالةِ فيها 512 بتًّا، وإذا زادَتْ عن ذلك فستقومُ بتقسيمِ الرِّسالةِ إلى أكثرَ مِنْ كتلةٍ (Block). أمَّا إذا نقصَتْ عَنْ ذلك فستَخضَعُ

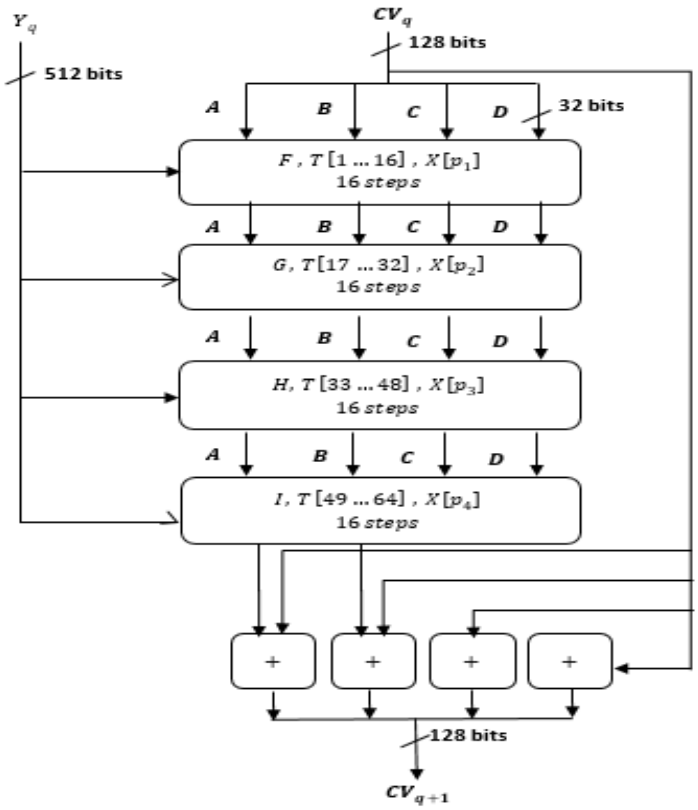
للمُعالجةِ بعمليَّاتِ الـ Padding[1] (الحشو). مِن الجديرِ بالذِّكرِ أنَّ المُخرَجَاتِ سوفَ تكونُ 128 بتًّا فقط، لهذا السَّببِ فإنَّ خَوارِزْميَّةَ الـ $MD5$ هي خَوارِزْميَّةُ تشفيرِ طولِ مِفتاحِها 128 بتًّا كَمَا في الشَّكلِ (1).



الشّكلُ (1): البناءُ الخارجيُّ لخوارزميَّةِ الـ MD5.

بعدَ أنْ يتُمَّ تقسيمُ الرِّسالةِ إلى كُتَلٍ سيتمُّ إرسالُ الكُتلةِ الأُولى إلى الـ buffer. الذي يكونُ فيهِ أربعةَ مُستطيلاتٍ مُتَموضِعَةً فوقَ بعضِها وتُسمَّى بالجولةِ (ROUND). في كلِّ جولةٍ تدخلُ البياناتُ في معالجةٍ تمُرُّ بـ 16 خطوةً (16 Step). من الجدير بالذكر أن كلُّ الخطواتِ لها الخوارزميَّةُ نفسُها كما في الشّكلِ (2).

Padding[1]**:** هي مجموعةُ من البتَّاتِ تُوضَعُ في آخرِ الرِّسالةِ إذا كانَ طولُ الرِّسالةِ أقصرَ مِنْ Block Size Message الذي يتحمَّلُهُ هذا النَّوعُ مِنَ التَّشفيرِ، ولا بُدَّ مِنْ وجودِهِ على الأقلِّ بـ 1 بتْ وعلى الأكثرِ 512 بتًّا.



الشَّكلُ (2): المعالجةُ داخلَ الـ Buffer في خوارزميَّةِ الـ MD5.

سنقومُ الآنَ بتوضيحِ مفهومِ الجولةِ بشيءٍ مِن التَّفصيلِ، وسوفَ نتعمَّقُ داخلَها لِنرى الخطوةَ.

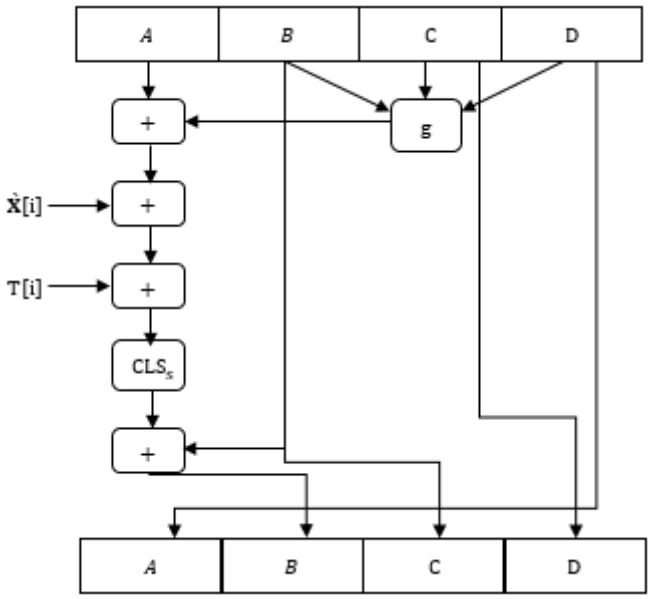
الـجَوْلَةُ:

هُناكَ أربعُ جولاتٍ في كُلِّ Buffer، وجميعُها لها الخَوارزميَّةُ نفسُها، لكنْ تختلفُ عن بعضِها في أنَّها تستخدمُ دوالّاً بوليانيَّةً مختلفةً، مثل: (F, G, H, I) فقِيَمُ تلكَ الدَّوَالِّ مُختلفةٌ، وبِنَاؤُهَا الدَّاخلِيُّ هُوَ عِبَارةٌ عن 16 خطوةً، كلُّ جولةٍ تأخذُ مدخلاتٍ حجمُها 512 بتًّا مِن Y_q ، قيمةُ Y_q هِيَ الرِّسالةُ المُقسَّمةُ، حيثُ إنَّ الرِّسالةَ تُقسَمُ إلى كُتَلٍ كلُّ واحدةٍ حجمُها 512 بتًّا، تدخلُ قيمةُ الـ Y_q والَّتي حجمُها 512 بتًّا على الجولةِ معَ دخولِ قِيَمِ (A, B, C, D)، والَّتي مجموعُ قيمِها 128 بتًّا، وإنَّ قيمةَ Y_q تكونُ ثابتةً في كلِّ الجولاتِ الأربعِ لـ $H_{MD5}buffer^2$ الواحدِ، وتختلفُ طبعاً مِن كلِّ $H_{MD5}buffer$، والَّذي يليه بسببِ اختلافِ قيمةِ جزءِ الرِّسالةِ، في الجولةِ: T دالَّةٌ حقيقيَّةٌ مجموعةُ قِيَمِها تُقدَّرُ بالرَّاديانِ وتُعطَى بالشَّكلِ الآتي:

$$T[i] = 2^{32} * abs(sin(i)) \; ; i = 1 \dots 64$$

إنَّ كلَّ جولةٍ تمتَلِكُ ترتيباً تسلسُلِيًّا مِن الخطواتِ موجودة في الـ buffer . وهذهِ الخطواتُ تخضَعُ للمُعادَلةِ الآتيةِ: $B = B + \left(\left(A + g(B, C, D) + \grave{X}[i] + T[i] \right) \ll s \right)$

إنَّ خوارزميَّةَ معادلةِ حسابِ الخطوةِ هذهِ نجدُها في الشَّكلِ (3).



الشَّكلُ (3): معادلةُ حسابِ الخطوةِ لخوارزميَّةِ MD5 الأصليَّةِ.

حَيثُ:

المقاديرُ: $\boldsymbol{A, B, C, D}$: هي المساحاتُ التَّخزِينيَّةُ المُؤقَّتةُ الَّتي تُستخدَمُ بترتيبٍ مُحدَّدٍ في كلِّ Step (خطوة).

g: هِيَ إحدى الدَّوالِّ (F, G, H, I) البوليانيَّةِ المتغيِّرةِ حسب كلِّ جولةٍ وتُـحسَـبُ مِنَ الجدولِ (2).

s »: اتِّجاهُ الإزاحةِ مِن اليَسارِ إلى اليمينِ بمِقدارِ **s** .

[i]X̀: بياناتُ رسالةٍ لكلِّ كتلةٍ وتحتوي على 512 بتًّا مُقسَّمةٍ إلى 16 كتلةً وحجمُ كلِّ منها 32 بتًّا.

CLS_s(Circular Left Shift): إزاحةٌ دائريَّةٌ لليَسَارِ بمِقْدَارِ s بت.

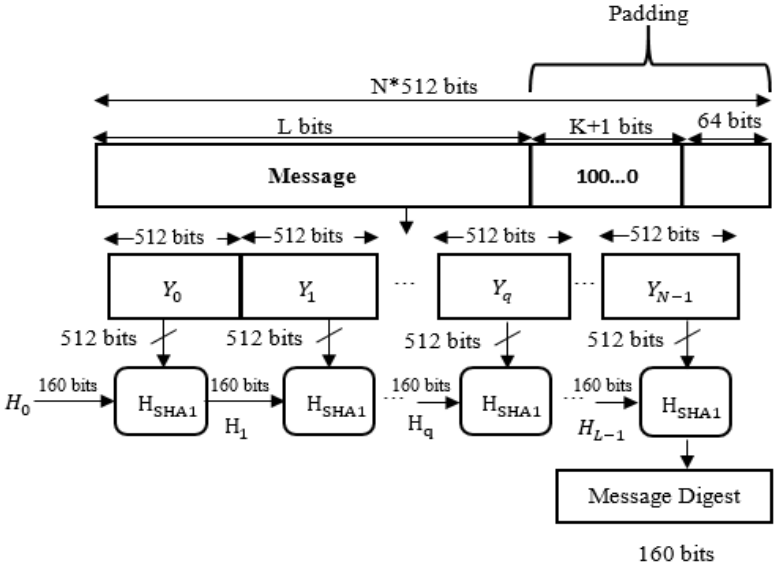
الجدولُ (2): دالَّةُ الجوْلاتِ وفْقَ الخَوارِزْميَّةِ الأصليَّةِ.

ROUND	Step	Primitive Function g	g (B, C, D)
1	1…16	F (B, C, D)	(B and C) or (not B and D)
2	17…32	G (B, C, D)	(B and D) or (C and not D)
3	33…48	H (B, C, D)	B XOR C XOR D
4	49…64	I (B, C, D)	C XOR (B or not D)

بعدَ إتمامِ كلِّ العمليَّاتِ السَّابقةِ على كلِّ أجزاءِ الرِّسالةِ فإنَّ خَرْجَ الخوارزميَّةِ سيكونُ عبارةً عن 128 بتًّا، هذا ما يُعرَفُ بـ **Message Digest**.

3-2-2 خوارزميَّةُ البَصْمةِ الآمنةِ (Secure Hash Algorithm 1, SHA 1)

صُمِّمَتْ خوارزميَّةُ SHA – 1 مِن قِبَلِ المَركزِ الوَطَنِيّ للمعاييرِ والتُّكنولوجيا NIST معَ وكالةِ الأمْنِ القوميّ بُغيةَ استخدامِها في التَّوقيعِ الرقميّ، فتأخُذُ خوارزميَّةُ SHA 1 رسائلَ بأطوالٍ غيرِ مُحدَّدةٍ، وتُعطِي على الخَرْجِ بصمةً بطولٍ ثابتٍ 160 بتًّا، ومِنْ ناحيةِ المُدخَلاتِ يكونُ طُولُ الرِّسالَةِ فيها 512 بتًّا، إذا زادَتْ عن ذلكَ فستقومُ بتقسيمِ الرِّسالةِ إلى أكثرَ مِنْ كُتلَة (Block)، أمَّا إذا نقصَتْ عن ذلكَ فستخضَعُ للمُعَالَجَةِ بعمليَّاتِ الـ Padding. ومِنَ الجَدِيرِ بالذِّكْرِ أنَّ المُخرَجَاتِ سوفَ تكونُ 160 بتًّا فَقَطْ، لذلكَ فإنَّ خوارزميَّةَ SHA – 1 هِيَ خوارزميَّةُ تَشفيرٍ طُولُ مِفتاحِها 160 بتًّا كَما في الشَّكلِ (4).



الشَّكلُ (4): البناءُ الخارجيُّ لخوارزميَّةِ SHA – 1.

بعدَ أنْ يتمَّ تقسيمُ الرِّسالةِ إلى كُتَلٍ سيتُمُّ إرسَالُ بياناتِ الكُتلةِ الأولى إلى الـ buffer الَّذي سوفَ تَتُمُّ المعالجةُ داخلَهُ، حيثُ نجِدُ أنَّ هُناكَ أربعةَ مُستطيلاتٍ مُتمَوضِعَةً فوقَ بعضِها وتُسمَّى المَرحلةَ $(Stage)$، جميعُها لها البِنيةُ الهيكليَّةُ ذاتُها ولكنَّها تختلفُ بالتَّوابعِ الدَّاخليَّةِ f_t والثَّوابتِ K_t (حيثُ $1 \le t \le 4$). تَتَكَوَّنُ كُلُّ مَرحَلةٍ مِن 20 جولةً، حيثُ تتُمُّ مُعالَجَةُ أجزاءٍ مِنْ كُتلةِ الرِّسَالةِ بوسَاطةِ التَّابعِ f_t معَ ثابتِ المَرْحلةِ K_t الَّذي يُعطَى بالعَلاقةِ الآتيةِ:

$$K_t = 512 - 64 - 1 - L = 448 - (L+1) mod\ 512.$$

يُضافُ الخَرْجُ بعْدَ 80 جولةً إلى القيمةِ المُدخَلةِ $H_{q-1} mod\ 2^{32}$، وسنقومُ الآنَ بتوضيحِ مفهومِ المَرحَلَةِ بشيءٍ مِنَ التَّفصيلِ، وسوفَ نتعمَّقُ داخلَها لِنرى الجولةَ.

المَرْحلَةُ:

هناكَ أربعُ مراحلَ في كلِّ Buffer، وجميعُها لها الخوارزميَّةُ نفسُها، لكنْ تختلفُ عن بعضِها في أنَّها تَستخدِمُ دوالَّ وثوابتَ مختلفةً، مثل: (f_t, k_t, W_j) حيثُ $j = 0 \dots 79$ ، قِيَمُ تلكَ الدَّوَالِّ مختلفةٌ، بناؤُها الدَّاخليُّ هُوَ عبارةٌ عن 20 جولةً، كلُّ جولةٍ تأخذُ مدخلاتٍ حَجْمُها 512 بتًّا من Y_q، قيمةُ Y_q هِيَ الرِّسالةُ المقسَّمةُ، حيثُ إنَّ الرِّسالةَ تُقسَمُ إلى كُتَلٍ كلُّ واحدةٍ حجمُها 512 بتًّا، تدخلُ قيمةُ الـ Y_q والَّتي حجمُها 512 بتًّا على المرحلةِ معَ دخولِ قِيَمِ (A, B, C, D, E)، والَّتي مجموعُ قيمِها 160 بتًّا، وإنَّ قيمةَ Y_q تكونُ ثابتةً في المَرَاحِلِ الأربعِ كلِّها لـ H_{SHA-1}buffer الواحد، وتختلفُ طبعاً مِنْ كلِّ H_{SHA-1}buffer، والَّذي يليه بسببِ اختلافِ قيمةِ جُزءِ الرِّسالةِ، في المرحلةِ: W دالَّةٌ تُعطَى بالشَّكلِ الآتي:

$$W_j = \begin{cases} Y_q & ; 0 \le j \le 15 \\ (W_{j-16} \text{ XOR } W_{j-14} \text{ XOR } W_{j-8} \text{ XOR } W_{j-3}) \ll 1 & ; 16 \le j \le 79 \end{cases}$$

إنَّ كلَّ مرحلةٍ تمتلكُ ترتيباً تسلسليّاً مِن الجولاتِ موجودة في الـ buffer ، وهذهِ الجولاتُ تخضعُ للمعادلةِ الآتية:

$$(A, B, C, D, E) = ((E + f_t(B, C, D) + (A) \ll 5 + W_j + K_t), A, (B) \ll 30, C, D)$$

حيث:

f_t: هِيَ إحدى الدَّوالِّ (f_1, f_2, f_3, f_4) المتغيّرةِ حسبَ كلِّ مرحلةٍ وتُحسَبُ وفْقَ الجدولِ (3).

≪: اتِّجاهُ الإزاحةِ مِنَ اليسارِ إلى اليمينِ.

الجدولُ (3): دوالُّ الجولاتِ وثوابتُها في خوارزميَّةِ SHA − 1 .

Stage t	ROUND	Constant K_t	Function f_t
1	0 ... 19	$K_1 = 5A827999$	$f_1(B, C, D) = (B \wedge C) \vee (B \wedge D)$
2	20 ... 39	$K_2 = 6ED9EBA1$	$f_2(B, C, D) = B \text{ XOR } C \text{ XOR } D$
3	40 ... 59	$K_3 = 8F1BBCDC$	$f_3(B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$
4	60 ... 79	$K_4 = CA62C2D6$	$f_4(B, C, D) = B \text{ XOR } C \text{ XOR } D$

بعدَ إتمامِ العمليَّاتِ السَّابقةِ كلِّها على أجزاءِ الرِّسالةِ كافَّةً، فإنَّ خَرْجَ الخوارزميَّةِ سيكونُ عبارةً عن 160 بتًّا.

4. توصيفُ النَّموذَجِ

4-1-خوارزميَّةُ MD5 المُعدَّلةُ (MMD5)

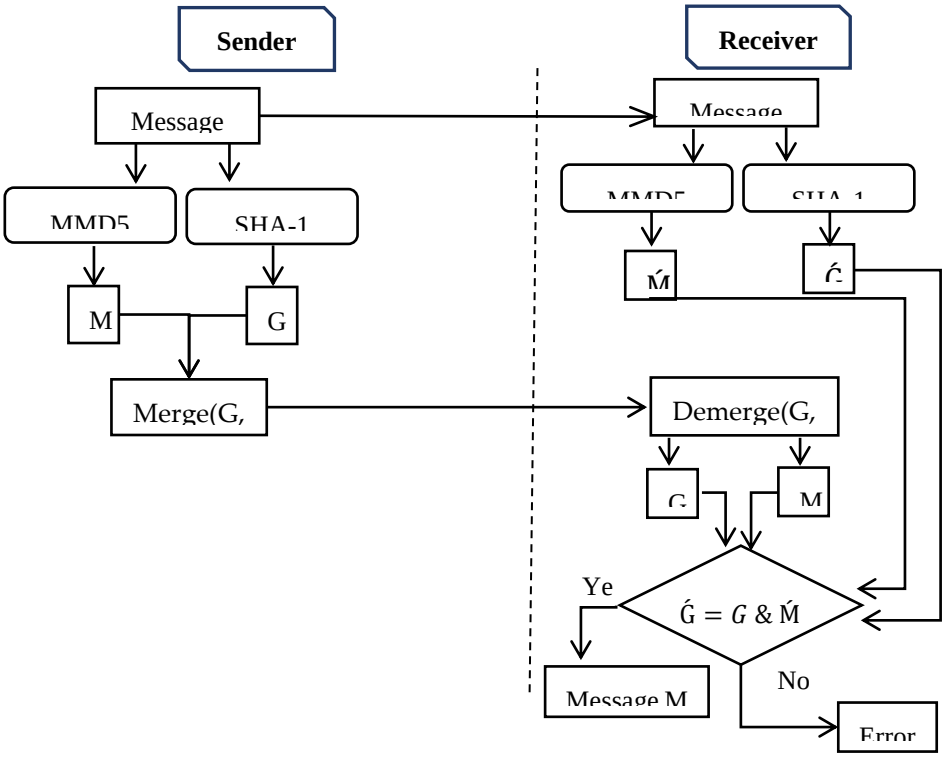
قُمْنا في هذا البحثِ بإجراءِ تعديلًا على خوارزميَّةِ MD5 وأطلقْنا عليها اسمَ MMD5. ومِن أجلِ تقليلِ زَمَنِ تنفيذِ خوارزميَّةِ MD5 قُمْنا بإجراءِ تعديلًا على العمليَّاتِ المنطقيَّةِ في معادلةِ حسابِ الخُطوة مع المحافظةِ على ، حيثُ استبدلْنا الـ XOR بالـ OR . كما قمْنا بتغييرِ اتِّجاهِ الإزاحةِ مِن اليسارِ إلى اليمينِ. الجدولُ (4) يوضِّحُ التَّعديلاتِ الَّتي قُمْنا بإجرائِها على العمليَّاتِ المنطقيَّةِ:

الجدولُ (4): دالَّةُ الجوّلاتِ وفْقَ الخوارزميَّةِ MMD5.

ROUND	Step	Primitive Function g	g (b, c, d)
1	1…16	F (B, C, D)	(B or not C) or (not B or D)
2	17…32	G (B, C, D)	(B or D) or (C or not D)
3	33…48	H (B, C, D)	not B or (not C or D)
4	49…64	I (B, C, D)	not C or (B or D)

4-2- النَّموذجُ المُقترَحُ

نُقدِّمُ في نموذجِنا المُقترَحِ هذا آليَّةً جديدةً لحمايةِ الرَّسائلِ المُرسَلةِ عبرَ الشَّبكةِ ومَنْعِ التَّلاعُبِ بِهَا، وإنَّ نموذجَنا المُقترَحَ يعتمدُ على دَمْجِ خوارزميَّتِنا المُعدَّلـةِ مَعَ خـوارزميَّتي تشفيرٍ، كَمَا في الشَّكلِ (5).



الشَّكلُ (5): آليَّةُ عَمَلِ النَّموذَجِ الَّذي قُمنا باقتراحِهِ.

يتألَّفُ نموذجُنا المُقترَحُ مِن قسمَينِ: قسمٌ خاصٌّ بالمُرسِلِ وآخَرُ خاصٌّ بالمُستقبِلِ، حيثُ يقومُ المُرسِلُ بتشفيرِ الرِّسالَةِ المُرَادِ إرسالُها مرَّتَينِ، **الأُولى:** باستِخدامِ خوارزميَّةِ MMD5 والحصولِ على البَصْمةِ M بطولِ 128 بتًّا. أمَّا **الثَّانيةُ:** باستِخدامِ خوارزميَّةِ SHA-1 والحصولِ على بصمةِ G بطولِ 160 بتًّا. بعدَ عملية التشفير يقومُ بدَمْجِ البَصمتَينِ M وG والحصولِ على ناتِجِ الدَّمْج بطولِ 128+160 بتاً. ثم يقُومُ المُرسِلُ بإرسالِ الرِّسالةِ الأصليَّةِ وناتِجِ الدَّمْجِ إلى المُستقبِلِ الَّذي بدورِهِ سيقومُ بتشفيرِ الرِّسالةِ الأصليَّةِ على مرحلتين: **الأُولى** باستخدامِ خوارزميَّةِ MMD5 والحصولِ على البَصْمةِ M̀ بطولِ 128 بتًّا. أمَّا **الثَّانيةُ** باستِخدامِ خوارزميَّةِ SHA-1 والحصولِ على بصمةِ Ġ بطُولِ 160 بتًّا. ثُمَّ يقومُ بِفَكِّ ناتِجِ الدَّمْجِ الَّذي أرسلَهُ المُرسِلُ والحصولِ على البصمتَينِ M وG. أخيرًا تتُمُّ مُقَارنةٌ بينَ البَصماتِ (M̀ وM و Ġ وG) للتَّحقُّقِ مِن استيقانِ وسرِّيَّةِ الرِّسالةِ المُرسَلَةِ، بهَدَفِ التَّصدِّي لِبعضِ الهَجماتِ كهُجُومِ التَّحليلِ الإحصائِيِّ وهُجُومِ المُقابلةِ في المنتصَفِ وهُجُومِ التَّزويرِ وهُجُومِ تعديلِ المُحتوَى، فإذا تحقَّقَ شَرْطُ التَّطابُقِ (G=Ġ & M=M̀) عندَئِذٍ ستَظْهَرُ على الشَّاشَةِ الرِّسَالةُ الأصلِيَّةُ. إذا لم يَتَحَقَّقْ شَرْطُ التَّطابُقِ فسوفَ تظهَرُ على الشَّاشةِ كلمةُ Error، **وهذا الظُّهُور يعني** أنَّهُ تَمَّ التَّلاعُبُ بالرِّسالةِ المُرسَلةِ مِن قِبَلِ مُهَاجِمٍ.

يُمكنُ توضيحُ آليَّةِ عَمَلِ نموذجِنا المُقترَحِ بمجموعةٍ من الخطواتِ؛ حيثُ تمَّ تقسيمُهَا إلى خطواتٍ خاصَّةٍ بالمُرسَلِ وأخرى خاصَّةٍ بالمُستقبِل. سنقومُ بشَرْحِ هذه الخطواتِ بالتَّفصيلِ كَمَا يَلِي:

خُطواتُ المُرسِلِ: يَقُومُ المُرسِلُ بالخطواتِ الآتية:

1- تشفيرُ الرِّسالةِ الأصليَّةِ باستخدامِ خوارزميَّةِ MMD5 والحصولِ على البَصْمةِ M بطولِ 128 بتًّا.

2- تشفيرُ الرِّسالةِ الأصليَّةِ باستِخدامِ خوارزميَّةِ SHA-1 والحصولِ على بصمةِ G بطولِ 160 بتًّا.

3- دمْجُ البصمتَينِ M وG برسالةٍ واحدةٍ وإعادةِ التَّرتيبِ.

خطواتُ المُستقبِلِ: يقومُ المُستقبِلُ بالخطواتِ الآتية:

1-تشفيرُ الرِّسالةِ الأصليةِ باستخدامِ خوارزميَّةِ MMD5 والحصولِ على البصمةِ M̀ بطولِ 128 بتًّا.

2-تشفيرُ الرِّسالةِ الأصليَّةِ باستخدامِ خوارزميَّةِ SHA-1 والحصولِ على بصمةِ Ġ بطولِ 160 بتًّا.

3-فكُّ الدَّمْجِ والحصولُ على البصمتَينِ M وG.

4- مقارنةُ البصماتِ (Ḿ و M و Ǵ و G) فإذا تحقَّقَ شرطُ التَّطابُقِ (G=Ǵ & M=Ḿ) عندئذٍ ستظهرُ على الشَّاشةِ الرِّسالةُ الأصليَّةُ، وإذا لم يتحقَّقْ شرطُ التَّطابُقِ فسوفَ تظهرُ على الشَّاشةِ كلمةُ Error وظهورُها يعني أنَّهُ تمَّ التَّلاعُبُ بالرِّسالةِ المُرسَلَةِ مِن قِبَلِ مُهاجِمٍ.

5. النَّتائِجُ والمُناقَشةُ (Results and Discussion)

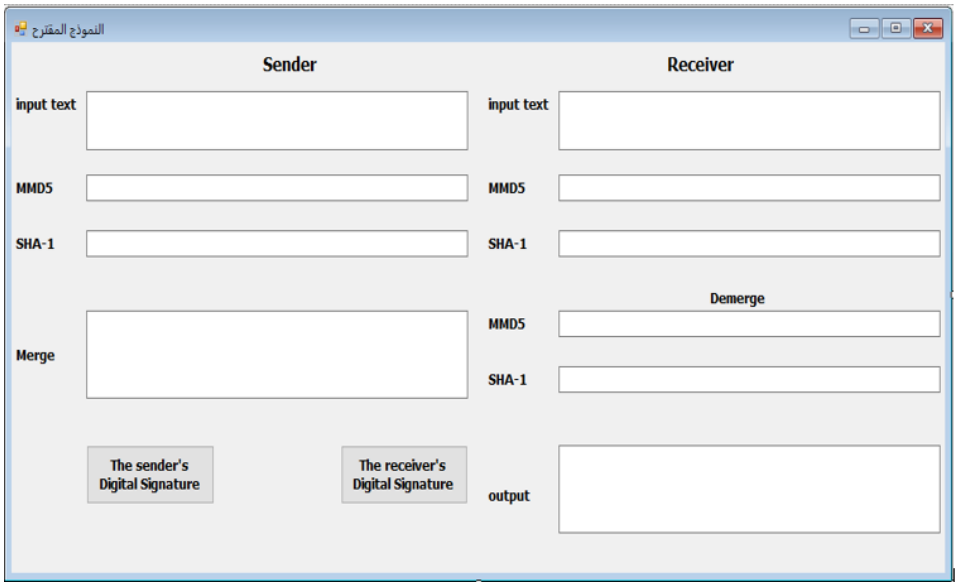
لتقييمِ كفاءةِ خوارزميّتِنا المُعدَّلةِ (MMD5)، سنستخدمُ لُغةَ C# بهدفِ إجراءِ محاكاةٍ للنَّتائجِ التَّجريبيَّةِ الَّتي توصَّلْنا إليها خلالَ بحثِنا، وفقَ المرحلتَينِ الآتيتَينِ:

المرحلةُ الأولى: تقليلُ زمَنِ تنفيذِ خَوارِزْمِيَّةِ الـ MD5 وذلكَ بتطبيقِها على عيّنةٍ من النّصوصِ. تَمَّ ذلكَ في نموذجِنا المُقترحِ من خلال تغييرِ بعضِ العَمَلِيَّاتِ المَنْطِقِيَّةِ وتغييرِ اتِّجَاهِ الإزاحة.

المرحلةُ الثَّانيةُ: زيادةُ استيقانِ الرَّسائلِ المُرسلةِ. تَمَّ ذلكَ في نموذجِنا المُقترحِ الَّذي يعتمدُ على عمليَّةِ الدَّمْجِ بينَ خوارزميَّتِنا المُعدَّلَةِ وخوارزميَّةِ الـ SHA-1.

مثالٌ تطبيقيٌّ

نعرضُ في هذا المثالِ آليَّةَ عَمَلِ نموذجِنا المُقترحِ، حيثُ قُمْنا بكِتَابةِ كودِ نموذجِنا المُقترَحِ في برنامجِ *Visual Studio* 2019 بلغةِ *C#* وتنفيذِه كمَا هو مُوضَّحٌ في الشَّكلِ (6):

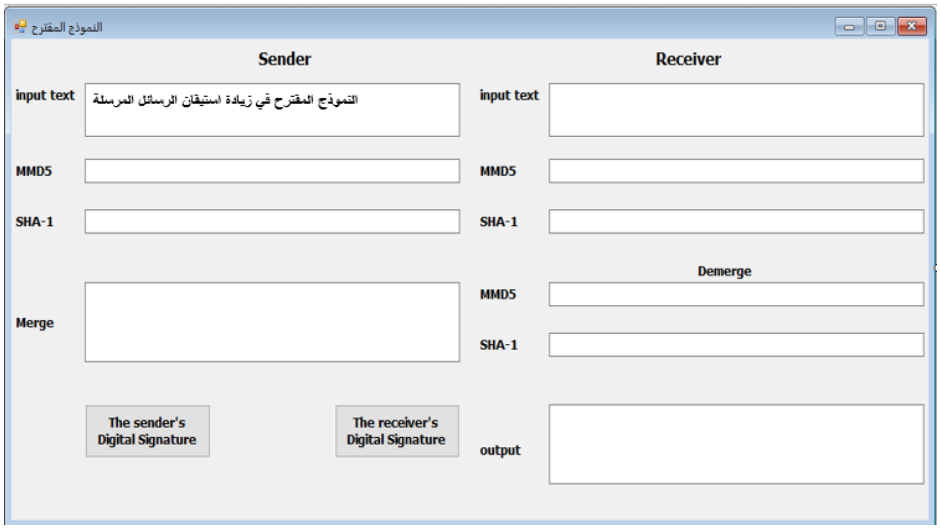


الشكل (6): واجهة النموذج الذي قمنا باقتراحه.

يُبيّنُ الشَّكلُ (6) أنَّ نموذجَنا المُقترَحَ ينقسمُ إلى قسمَينِ؛ قسمٌ خاصٌّ بالمُستقبِلِ وقسمٌ خاصٌّ بالمُرسِلِ كَما يأتي:

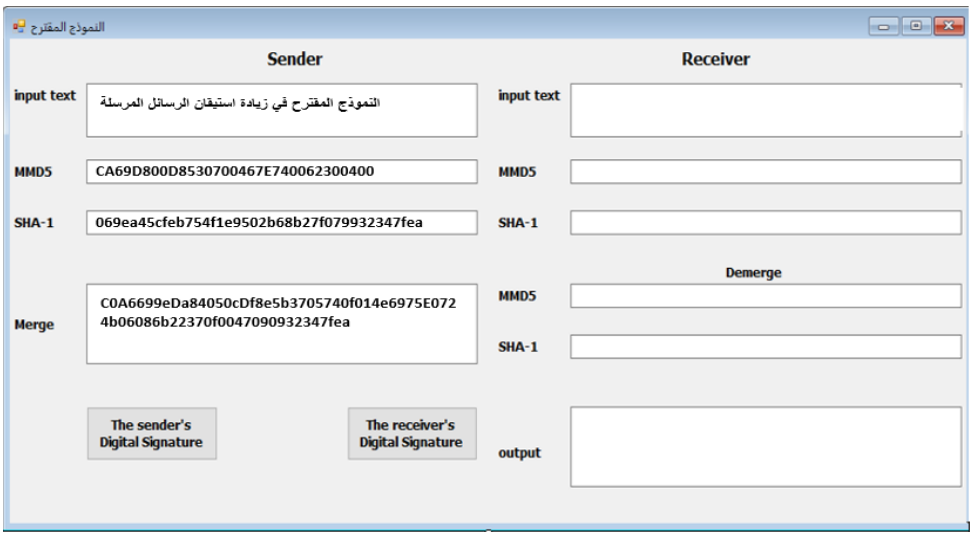
1- قسمُ المُرسِلِ:

يقومُ المُرسِلُ بكتابةِ الرّسالةِ المُرادِ إرسالُها في الحقلِ *input text* كَمَا في الشَّكلِ (7).



الشَّكلُ (7): عمليَّةُ إدخالِ الرّسالةِ المُرادِ إرسالُها.

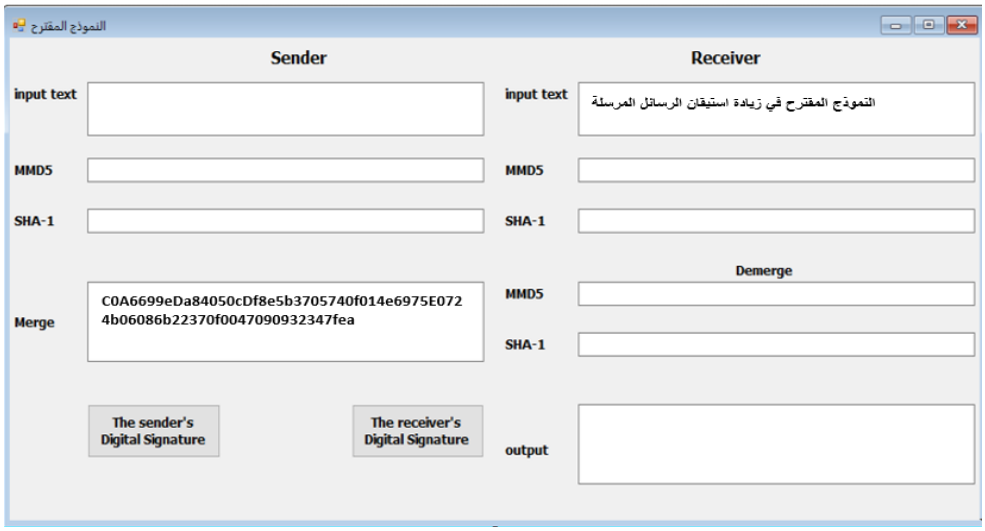
يقومُ المُرسِلُ بالضَّغطِ على زرِّ *The sender's Digital Signature* فتتُمُّ عمليَّةُ تشفيرِ النَّصّ المُدخَلِ بوساطةِ الخوارزميَّتَينِ MMD5 و SHA-1 والحصولِ على بصمتَي الخوارزميَّتَينِ MMD5 و SHA-1 وإظهارِ ناتِجِ الدَّمْجِ في الحقْلِ Merge كمَا في الشَّكلِ (8). ثُمَّ يقومُ المُرسِلُ بإرسالِ الرّسالةِ الأصليَّةِ معَ ناتِجِ الدَمْجِ إلى المُستقبِلِ.



الشَّكل (8): عمليتَا التَّوقيعِ الرَّقْمِيّ والدَّمْجِ.

2-قِسمُ المُستقبِلِ

يقومُ المُستقبِلُ باستقبالِ الرّسالةِ الأصليَّةِ معَ ناتِجِ الدَّمْجِ ووضعِهما في المكانِ المُخصَّصِ لهما كمَا في الشَّكلِ (9).

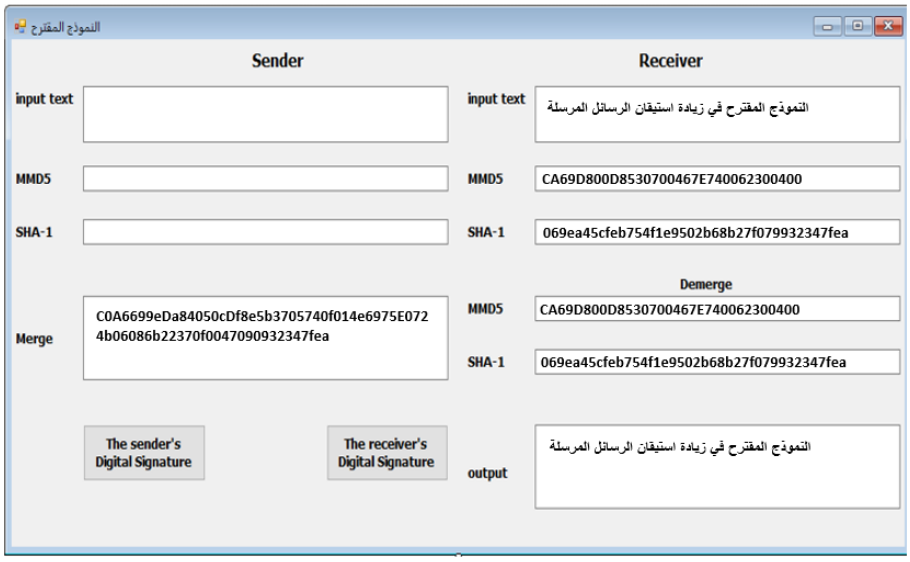


الشَّكلُ (9): عمليَّةُ وَضْعِ النَّصِ الأصليّ معَ ناتجِ الدَّمْجِ.

يقومُ المُستقبِلُ بالضَّغطِ على زرِ *The receiver's Digital Signature* فيقومُ البرنامجُ بتشفيرِ النَّصِّ المُدخَلِ بوساطةِ الخوارزمِيَّتَينِ MMD5 و SHA-1 والحصولِ على بصمتَي الخوارزميَّتَينِ MMD5 و SHA-1. ثُمَّ يقومُ بفكِّ دَمْجِ البصمتَينِ والحصولِ على البصمتَينِ الأساسيَّتَينِ ووضعِهما في الحقلَينِ MMD5 و SHA-1 التَّابعَينِ للعمليَّةِ Demerge.

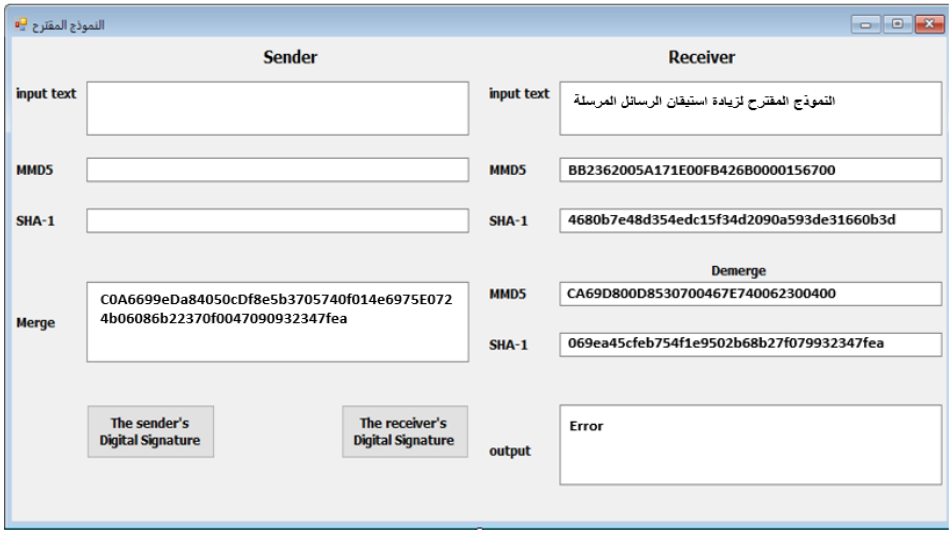
أخيرًا يتمُّ إجراءُ مقارنةٍ بينَ بصمتَي MMD5 النَّاتجتَينِ عن تشفيرِ المُستقبِلِ وفكِّ الدَّمْجِ، ومُقارنةِ بصمتَي SHA-1 النَّاتجتَينِ عَنْ تشفيرِ المُستقبِلِ وفَكِّ الدَّمْجِ، وهُنا نُميِّزُ حالتَينِ:

<u>الحالةُ الأولى</u>: إذا كانَتِ بصمَتَا المُستقبِلِ والمُرسِلِ لخوارزميَّةِ الـ MMD5 متطابقتَينِ وبصمَتَا المستقبلِ والمُرسِلِ لخوارزميَّةِ الـ-SHA 1 متطابقتَينِ. عندَئذٍ يتُمُّ إظهارُ الرِّسالةِ الأصليَّةِ في الحقلِ *output* كمَا في الشَّكلِ (10).



الشَّكلُ (10): عمليَّةُ التأكُّدِ مِنْ أصالةِ الرِّسالةِ الأصليَّة.

<u>الحالةُ الثَّانيةُ</u>: كما نُلاحِظُ في الشَّكلِ (11) استبدلْنا بحرفِ الجرِّ (في) حرفَ الجرِّ (اللَّام) في الرِّسالةِ الأصليَّةِ بالقِسمِ الخَاصِّ بالمُستقبِلِ وذلكَ لتوضيحِ كيفيَّةِ كشفِ العَبَثِ في الرِّسالةِ الأصليَّةِ مِنْ طَرَفٍ ثالثٍ. إذا كانَتْ بصمَتَا المُستقبِلِ والمُرسِلِ لخوارزميَّةِ الـ MMD5 مختلفتَينِ أو بصمَتَا المُستقبِلِ والمُرسِلِ لخوارزميَّةِ الـ SHA-1 مختلفتَينِ. عندَئِذٍ يتُمُّ تنبيهُ المُستخدمِ بذلكَ وإظهارُ الكلمةِ Error في الحقلِ *output*.



الشَّكلُ (11): إظهار عبارة "Error" لتنبيهِ المُستخدمِ.

6. الاستِنتاجاتُ والتَّوصياتُ (Conclusions and Recommendations)

مِنْ خلالِ بحثنا هذا توصَّلْنا إلى الاستِنتاجاتِ الآتيةِ:

1- تعديلُ خوارزميَّةِ الـ MD5 وذلكَ بهدفِ التَّقليلِ مِنْ زَمَنِ تنفيذِها.

2- بناءُ نموذجٍ مُقتَرَحٍ يعتمدُ على خوارزميتِنا المُعدَّلةِ ودمجِها معَ خوارزميَّةِ التَّوقيعِ الرَّقْميّ SHA-1، وذلكَ لزيادةِ استِيقانِ الرَّسائلِ المُرسَلَةِ وحمايتِهَا.

3- تطبيقُ نموذجِنا المُقترَحِ بمثالٍ توضيحيٍّ.

استكمالاً لنتائجِ البحثِ واستنتاجاتِهِ نُوصِي بما يلي:

1- إمكانيةُ التَّعديلِ على العلاماتِ المنطقيَّةِ في خوارزميَّتِنا مِنْ أجلِ الحصولِ على زمَنِ تنفيذٍ أقلَّ.

2- تطبيقُ خوارزميَّاتِ التَّوقيعِ الرَّقميّ لتعزيزِ الاستيقانِ والسَّلامةِ والسِّرِّيَّةِ للرَّسائلِ المُرسلةِ.

3- إمكانيَّةُ التَّعديلِ على نموذجِنا المُقترحِ وذلكَ بدَمْجِ خوارزميَّتِنا المُعدَّلةِ مَعَ أكثرَ مِنْ خوارزميَّةِ توقيعٍ رَقْمِيٍّ.

المَرَاجِعُ (References):

1. الخيرو، ماجد. الحلبي، محمد فراس. (2023). *دراسة لمنع التلاعب بالرسائل المشفرة عبر الشبكة باستخدام التوقيع الإلكتروني.* رسالة ماجستير. قسم الرياضيات. كلية العلوم. جامعة دمشق. دمشق: سوريا. ص:88.

2. ملكيه، حنان. مكناس، محمد. إسماعيل، محمد. (2010). النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري. *مجلة جامعة دمشق للعلوم الاقتصادية والقانونية*. المجلد:26. العدد:2. ص:549-573.

3. ALFRED J, MENEZES. PAUL C, VAN OORSCHOT, AND SCOTT A, VANSTONE. (1996). *Handbook of Applied Cryptography, CRC Press*.
4. Alkheirow. M. Alhalabi. M. (2022). A Study to Prevent Tampering with Encryption Messages over the Network using an Digital Signature. *Journal of Mathematics /Hindawi/.*
5. C. PAAR AND J. PELZL. (2010). Understanding Cryptography. pages 307-312, *Springer-Verlag Berlin Heidelberg.*
6. O. GOLDREICH, (2009) *Foundations of Cryptography Basic Applications*, Cambridge University Press.
7. OVIDIU. GHITA, (2003) *Binary-coded_decimal*, Digital Electronics, PP.77-**117.**
8. PRERNA MAHAJAN & ABHISHEK SACHDEVA. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security, *Global Journal of Computer Science and Technology Network, Web & Security* Volume 13 Issue 15 Version 1.0 Year.
9. W. STALLINGS, (2014). *Cryptography and Network Security, Principle and practice*.