مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١١) ٢٠٢٥

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (11) 2025

تحسين الخوارزمية الجينية المدمجة بالذكاء المحلي لتوليد مفاتيح تشفير آمنة في بيئات الحوسبة السحابية

د. راغب طعمة *

م. مرح محمد فسخه **

(تاريخ الإيداع ٢٠٢٥/٧/٣ . قُبِل للنشر في ٢٠٢٥/٩/١٤)

□ ملخّص □

في ظل الاعتماد المتزايد على تقنيات الحوسبة السحابية، تبرز الحاجة المُلِحَّة إلى حماية البيانات الحساسة من الهجمات السيبرانية المتزايدة. لذلك يمثل التشفير أحد الحلول الفعالة لضمان سرية وأمان البيانات السحابية. يعرض هذا البحث إطارا هجينا مبتكرا يجمع بين الخوارزمية الجينية التقليدية (Genetic Algorithm) ومبادئ خوارزمية الذكاء المحلي، والتي تعتمد على مزيج من المعلومات المحلية والعشوائية ضمن بنية رياضية، بهدف تحسين أداء الخوارزمية الجينية في توليد مفاتيح تشفير قوية وعشوائية (سواء التقليدية الثنائية أو تلك المعتمدة على الحمض النووي DNA) يمكن الاعتماد عليها ضمن مخططات التشفير الحديثة. تم تنفيذ المنهج الهجين المقترح ضمن سيناريوهين:

في السيناريو الأول، تم استخدام الخوارزمية الجينية المعدلة لتوليد مفاتيح ثنائية وتم تقييم جودتها من حيث العشوائية والتفرد. أظهرت النتائج أن 98.7% من المفاتيح ذات حجم 64 بت وصلت إلى أقصى قيمة للانتروبيا (1,0) ، وحققت 95% منهامتوسط مسافة هامينغ مقداره 32.02 ، ومعامل ارتباط منخفض جدًا (0.0005−) ، ما يدل على تميز المفاتيح من حيث العشوائية والتفرد، وقدرتها العالية على مقاومة الهجمات الأمنية.

أما في السيناريو الثاني، فقد تم تطبيق المنهج ذاته لتعزيز مفاتيح تشفير الحمض النووي(DNA−based keys) الضعيفة، التي تم توليدها عشوائيًا باستخدام قواعد نتروجينيه A, T, C, G. وأظهرت النتائج أن المنهج المقترح يساهم في تقليل الحاجة إلى عمليات تعزيز إضافية عبر تحسين اللياقة الوراثية تدريجيًا على مدى الأجيال المتعاقبة.

تشير النتائج الكلية إلى أن المنهجية الهجينة المُقترحة تحقق تفوقا واضحا في توليد مفاتيح آمنة، عشوائية، ومتفردة أي تعزز بشكل كبير جودة المفاتيح التشفيرية، وتزيد من مناعتها تجاه الهجمات الإحصائية وهجمات القوة الغاشمة، مما يجعلها مناسبة للتطبيق في أنظمة التشفير المعاصرة بما في ذلك الأمن السحابي وتشفير الحمض النووي.

الكلمات المفتاحية :الخوارزمية الجينية، خوارزمية الذكاء المحلي، التشفير، الحوسبة السحابية، تشفير الحمض النووي.

*مدرس في قسم تكنولوجيا المعلومات–كلية هندسة تكنولوجيا المعلومات والاتصالات–جامعة طرطوس –طرطوس–سوريا

** طالبة ماجستير في قسم تكنولوجيا المعلومات–كلية تكنولوجيا المعلومات والاتصالات–جامعة طرطوس –سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١١) ٢٠٢٥

Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (11) 2025

Enhancing the Genetic Algorithm Integrated with Local Intelligence for Secure Key Generation in Cloud Computing Environments

Dr.Ragheb Toemeh *

Eng.Marah mohammed faskha **

(Received 3/7/2025 . Accepted 14/9/2025)

□ **ABSTRACT** □

In light of the increasing reliance on cloud computing technologies, there is a pressing need to protect sensitive data from the growing threat of cyberattacks. Encryption thus represents one of the most effective solutions for ensuring the confidentiality and security of cloud-based data. This study proposes an innovative hybrid framework that combines the traditional Genetic Algorithm (GA) with the principles of a Local Intelligence Algorithm, which utilizes a blend of local and stochastic information within a mathematical structure. The goal is to enhance the performance of the GA in generating strong and random encryption keys—whether conventional binary keys or DNA-based keys—that can be reliably employed in modern cryptographic schemes.

The proposed hybrid approach was implemented in two scenarios:

In the first scenario, the modified GA was used to generate binary encryption keys, whose quality was evaluated in terms of randomness and uniqueness. The results showed that 98.7% of the 64-bit keys achieved the maximum entropy value (1.0), 95% achieved an average Hamming distance of 32.02, and exhibited an extremely low correlation coefficient (−0.0005), indicating that the keys were highly random, unique, and robust against security attacks.

In the second scenario, the same approach was applied to enhance weak, randomly generated DNA-based encryption keys using nucleotide bases A, T, C, and G. The results demonstrated that the proposed method contributed to reducing the need for additional strengthening operations by gradually improving the genetic fitness across successive generations.

Overall, the findings indicate that the proposed hybrid methodology clearly outperforms traditional approaches in generating secure, random, and unique keys. It significantly improves cryptographic key quality and enhances resistance against statistical and brute-force attacks, making it suitable for deployment in modern encryption systems, including cloud security and DNA cryptography.

Keywords: Genetic Algorithm, Local Intelligence Algorithm, Encryption, Cloud Computing, DNA Cryptography.

* Lecturer, Department of Information Technology, Faculty of Information and Communication Technology, University of Tartous, Syria

**Master student, Department of Information Technology, Faculty of Information and Communication Technology, University of Tartous, Syria

١- المقدمة (Introduction)

شهدت العقود الأخيرة نموًا هائلًا في تبادل البيانات الرقمية، معتمدًا بشكل ملحوظ على بنى الحوسبة السحابية لتخزينها ومعالجتها. إلا أن هذا التوسع أفرز تحديات أمنية خطيرة، أبرزها ضمان سرية وسلامة البيانات المخزنة والمنقولة عبر الخوادم السحابية. من أجل التصدّي لهذه التهديدات المتنامية، بات من الضروري اعتماد آليات تشفير متقدمة ومرنة لضمان حماية فعّالة لمعلومات المستخدمين.

في هذا السياق، حظي مجال التشفير الحيوي وبشكل خاص تشفير الحمض النووي (DNA Cryptography) باهتمام متزايد. حيث تكشف الدراسات الحديثة أن تكامل العمليات المستوحاة من خصائص الحمض النووي، مثل الإنزيمات والنماذج الجزيئية، يُساعد في زيادة التعقيد العشوائي للخوارزميات، وهو ما ينعكس في مستوى أعلى من الأمان وكفاءة تنفيذ منخفضة التكلفة، كما يتضمن استخدام أساليب تشفير مدمجة تعمل بكثرة على الأجهزة منخفضة المواصفات مثل Raspberry Pi [1].

إلى جانب ذلك، حظيت الخوارزميات التطورية وفي مقدمتها الخوارزميات الجينية (Genetic Algorithms, GA) باهتمام متزايد في مجال التشفير حيث أظهرت الدراسات الحديثة فعالية الخوارزميات الجينية عند دمجها في نظم التشفير السحابي. حيث طرحت الكثير من آليات التشفير المدعومة بالخوارزمية الجينية والتي تهدف إلى تعزيز أمان البيانات السحابية مع تحقيق زمن تشفير وفكّ أسرع ونجاح أعلى مقارنة بأساليب تقليدية [2]. بالإضافة لأساليب هجينة أخرى، تقدم إطارًا تشفيريًا متطورًا مقاومًا للتهديدات المستقبلية، عبر بناء نظم ديناميكية قادرة على التكيف وتحسين القدرة على التعمية ومرونة التصدي للهجمات [3].

من هذا المنطلق، يشير الجمع بين تشفير الحمض النووي والخوارزميات الجينية إلى إمكانيات واعدة لتعزيز أمن البيانات في البيئات السحابية: حيث تُقدّم الأولى القدرة على التعمية ذات درجة عالية وتنفيذ خفيف الموارد، في حين توفر الثانية توليد مفاتيح غامضة عالية التعقيد، وقابلية للتكيف والديناميكية في مواجهة التهديدات الحديثة. ويضع هذا التكامل الأساس لمنهجية تشفير مستقبلية تجمع بين الأمان، الفعالية، والابتكار في تعزيز الثقة الرقمية.

2- مشكلة البحث (Research problem)

نلخص مشكلة البحث كما يلي:

مع التوسع السريع في استخدام تقنيات الحوسبة السحابية، ازداد الاعتماد على تخزين البيانات الرقمية عبر الإنترنت، بما يشمل معلومات ذات طابع حساس وسري. هذا الاعتماد المتزايد أدى إلى تصاعد المخاوف الأمنية المرتبطة باحتمالية تعرض هذه البيانات للاختراق، أو التسريب، أو الوصول غير المصرح به من قبل جهات خارجية. تتمثل الإشكالية الرئيسة في الحاجة إلى آليات تشفير أكثر تطورًا تضمن أمن البيانات السحابية في ظل التحديات المتزايدة التي تفرضها بيئة الإنترنت الحديثة. وعلى وجه الخصوص، فإن التشفير التقليدي لم يعد كافيًا وحده لتوفير مستويات الأمان المطلوبة، مما يستدعي البحث في تحسين تقنيات التشفير الحالية من خلال اعتماد خوارزميات أكثر قدرة على توليد مفاتيح تشفير معقدة وعشوائية.

3-أهمية البحث وأهدافه (Importance of research and its objectives)

يمثل التشفير أحد الركائز الأساسية في حماية البيانات وضمان سرية المعلومات الرقمية، خاصة في بيئات الحوسبة السحابية التي تتطلب أنظمة أمان قوية. وتُعد قوة مفتاح التشفير وتعقيده من العوامل الحاسمة التي تحدد فعالية نظام التشفير ومدى مقاومته للهجمات. لذلك سيتم تعزيز قوة أنظمة التشفير من خلال غرس فوائد الخوارزمية الجينية في تقنيات التشفير (التشفير التقليدي وتشفير الحمض النووي) بناءً على ذلك، يهدف هذا البحث إلى تحسين أداء الخوارزمية الجينية في توليد مفاتيح تشفير ذات درجة عالية من العشوائية والتفرد، وذلك من خلال تطوير منهج هجيني يجمع بين الخوارزمية الجينية وخوارزمية محلية تعتمد على الذكاء.

وتتجسد أهداف البحث الأساسية فيما يلي:

١- تعزيز عشوائية مفاتيح التشفيرية الثنائية المنتَجة باستخدام الخوارزمية الجينية التقليدية، وذلك عبر دمجها مع خوارزمية الذكاء المحلي.

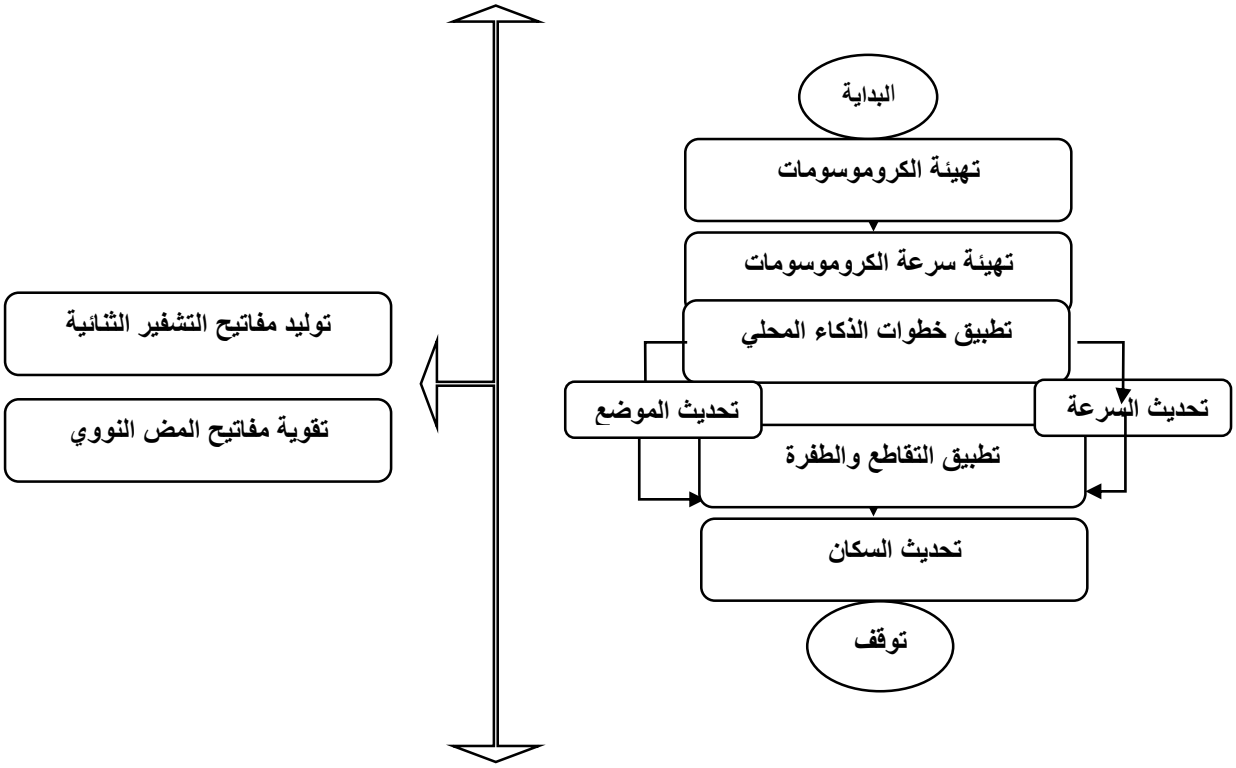
٢- تقوية مفاتيح الحمض النووي (DNA Keys) التي تقيّم على أنها ضعيفة، من خلال إعادة تهيئتها وتطويرها باستخدام المنهج الهجين، ما يتيح إمكانية إعادة استخدامها بدلًا من إهمالها.

٣- تحقيق توازن بين الأمان وكفاءة التوليد، بحيث يتم توليد مفاتيح قوية بأقل وقت ممكن ودون زيادة عبء الحوسبة بشكل غير فعّال.

يسعى هذا البحث إلى تقديم إطار تشفيري أكثر قوة وكفاءة يمكن تطبيقه في مختلف أنواع التشفير سواء التقليدي أو القائم على الحمض النووي، بما يدعم أمن المعلومات في البيئات الرقمية الحديثة.

4- طرائق البحث ومواده (Research methods and materials)

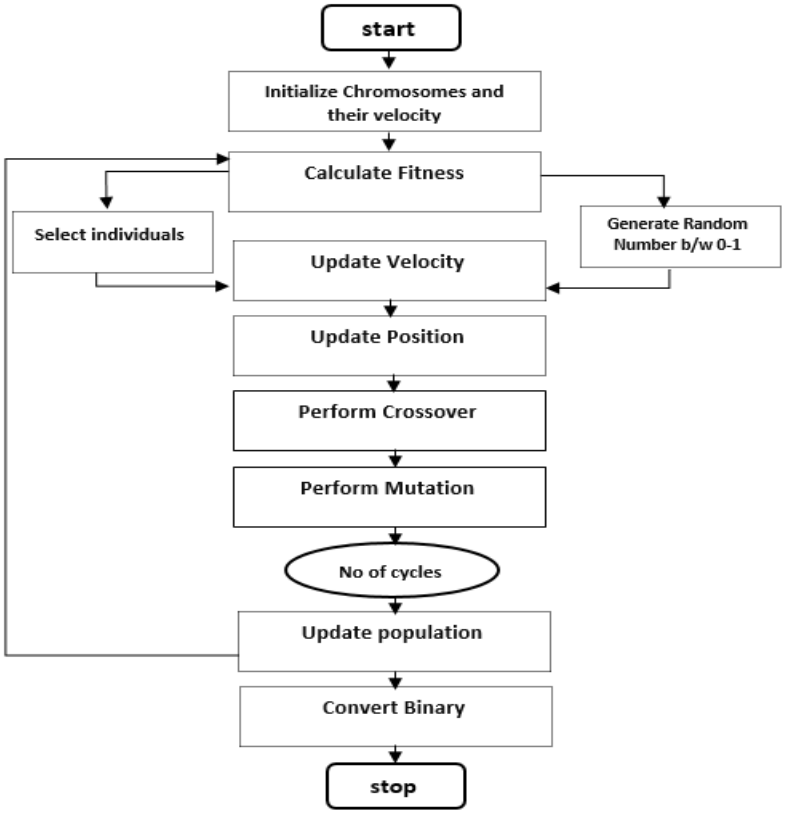
في هذا القسم سنعرض المنهجية العملية التي تم تطبيقها لاختبار فعالية الخوارزمية المقترحة، سيتم تنفيذ هذا البحث باستخدام لغة البرمجة python ، على جهاز حاسوب شخصي يمتلك وحدة معالجة مركزية ®intel corei3-6100u بسرعة 2.3 غيغاهرتز وذاكرة وصول عشوائي (RAM) 4 غيغابايت. تم التركيز في هذا المقال على تحسين توليد مفاتيح التشفير باستخدام الخوارزمية الجينية، وذلك من خلال دمجها مع خوارزمية محلية تعتمد على الذكاء (Local Intelligence-Based Algorithm) [4]، بهدف تعزيز قدرة الخوارزمية على توليد مفاتيح أكثر تعقيدًا وعشوائية. في هذا المقال سيتم تطبيق المنهجية الهجينة على مرحلتين أو وفق سيناريوهين: في المرحلة الأولى سنطبق المنهج الهجين للخوارزمية الجينية المعزز بالذكاء لتوليد مفاتيح تشفير ثنائية ونقيس أداء لمفاتيح المولدة وعشوائيتها لنقيس مدى فعالية هذا التحسين في التشفير الثنائي، لنعود في المرحلة الثانية ونطبق هذا المنهج في التشفير القائم على الحمض النووي وقياس مدى فعاليته في تقوية مفاتيح التشفير ذات تابع اللياقة الضعيفة. يوضح الشكل (1) الإطار العام للمنهجية المقترحة.



الشكل (1) منهجية للبحث

4-1 توليد مفاتيح التشفير الثنائية (Binary Key Generation):

في هذا القسم سيتم شرح مراحل السيناريو الأول من المنهجية المقترحة، بداية في هذه المرحلة سيتم تنفيذ الخوارزمية الجينية بخطوتيها الأساسيتان (التقاطع والطفرة) لتحسين لياقة الكروموسومات وتعزيزهم مع المنهج القائم على الذكاء (الذي يتضمن تحديثات السرعة للمفاتيح المنشأة (الكروموسومات) وتحديثات المواضع لهذه الكروموسومات). يبين الشكل (2) منهجية توليد مفاتيح التشفير الثنائية.



الشكل (2) منهجية توليد مفاتيح تشفير ثنائية

4-1-1 تهيئة الكروموسومات وسرعاتهم (Initialize Chromosomes and their) Velocity

بداية يتم تهيئة (إعداد) المجتمع الأولي من مجموعة من الكروموسومات بشكل عشوائي، كل كرموسوم (فرد) ضمن المجتمع يمثل مفتاح تشفير محتمل. كل كروموسوم يتكون من مجموعة من المكونات المتغيرة التي تسمى الجينات التي يتم ربطها في سلسلة ثنائية (تسلسل من الأصفار والواحدات) وهذه المرحلة تسمى تشفير الكروموسوم [5].

بعد ذلك سيتم تهيئة سرعات الكروموسومات، كل فرد سيتم تمثيله على شكل متجه سرعة (طول متجه السرعة من حجم الفرد أو الكروموسوم). أي سيتم تمثيل سرعة كل جين من الكروموسوم (تمثيل كل جين بقيمة عائمة) مما يسمح بإجراء تعديلات في موضع الجينات لاحقا. تشير سرعات الأفراد (Velocity) في هذه الخوارزمية، انه يوجد لكل "فرد" من السكان موضع في مساحة البحث، ويتغير هذا الموضع بمرور الوقت بناء على سرعة الفرد.

4-1-2 حساب تابع اللياقة باستخدام عجلة روليت (Roulette Wheel Selection)

سيتم اختيار فردين من السكان بناءً على لياقتهما. باستخدام عجلة الروليت للتحديد [6]، وهي طريقة احتمالية حيث يكون لدى الأفراد ذوي اللياقة العالية فرصة أكبر للاختيار. اللياقة هنا هي عدد الواحدات الموجودة في جينات الفرد المحددة. إذا كان جميع الأفراد يتمتعون بلياقة منخفضة، يصبح الاختيار أكثر عشوائية.

4-1-3 تحديث السرعة (Velocity Update)

بعد اختيار فردين (كروموسومين) بناءا على اختيار عجلة روليت سيتم تحديث سرعة الأفراد المختارين بإضافة بعض العشوائية لجينات هذه الأفراد (الكروموسومات). هذه المرحلة تتألف من خطوتين:

الخطوة1: توليد بت عشوائي: حيث أن البت العشوائي هو رقم عشوائي بين (0,1) سيتم إضافته لكل عنصر من عناصر متجه السرعة الخاص بالكروموسومين المختارين. تؤدي إضافة هذا البت العشوائي إلى سرعة الفرد لإدخال عشوائية إضافية في عملية التحديث، مما يجعل سرعة كل جين أكثر تغيرا عبر الأجيال.

الخطوة2: تحديث السرعة: سيتم استرجاع متجه السرعة الخاص بالفردين المختارين وتتم إضافة البت العشوائي الذي تم توليده في الخطوة السابقة لكل جين أو عنصر بمتجه سرعة الفرد (الكروموسوم). يتم تحديث هذه السرعات خلال كل تكرار ، وهي تؤثر على كيفية تحرك الفرد عبر مساحة الحل ، مما يسمح له بالبحث عن حلول أفضل.

4-1-4 تحديث الموضع (Position Update)

يتم تطبيق السرعة الجديدة على الموضع الحالي للفرد (الجينات) لتحريكه في اتجاه جديد. أي سيتم استخدام السرعة لتغيير موضع الفرد، سيتم استرجاع سرعة الجين للفرد وقيمة الجين الحالية. يتم حساب مجموع السرعة وقيمة الجين الحالية وتخزينها مرة أخرى في جينات الفرد المؤقتة. هذا يعني أن الجين (أو الموضع) الجديد للفرد يتأثر بالسرعة، مما يوجه مقدار تغير الجين في التكرار التالي.

يتم التحديث بناءا على الصيغة (3) التالية [4]:

$$v_{im}(n) = v_{im}(n) + (\varphi + X_{im}) \quad (3)$$

حيث:

$v_{im}(n)$ هي سرعة الجين m من الوالد i عند التكرار n

x_{im}هو الجين m من الوالد i

φ هي قيمة البت العشوائي.

4-1-5 تطبيق التقاطع (Perform Crossover)

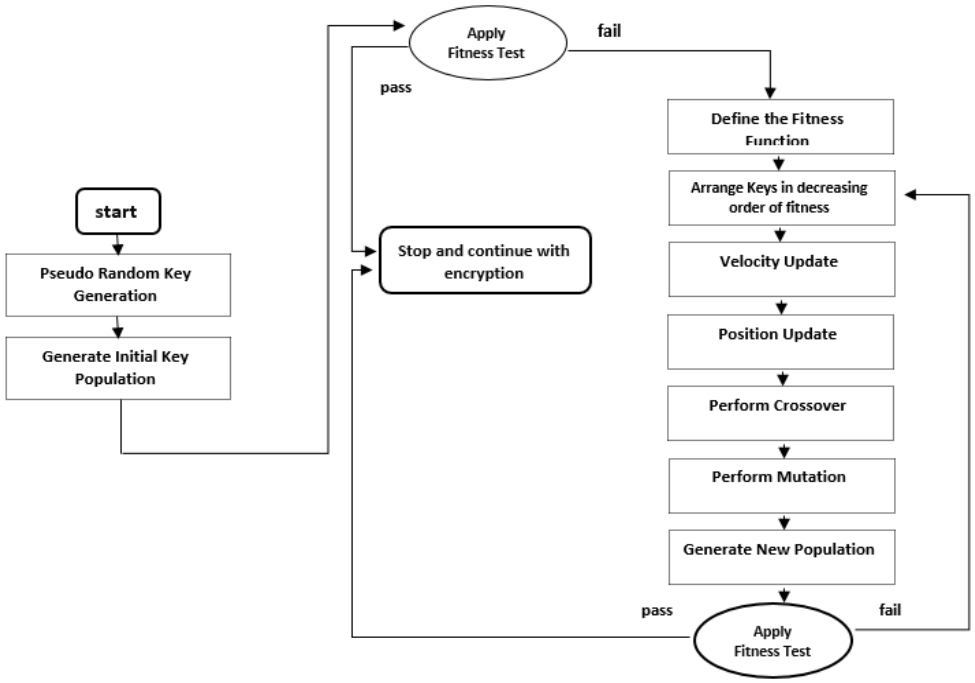
سيتم في هذه المرحلة تطبيق التقاطع من النوع Single-Point Crossover: تتم عملية تقاطع نقطة واحدة بين الفردين المختارين في الخطوة السابقة (مفاتيح ثنائية). بهدف الجمع بين المادة الوراثية لهذين الفردين (الوالدين) لإنشاء تنوع جيني في الجيل التالي. حيث سييتم اختيار نقطة التقاطع بشكل عشوائي بين (1,64). يضمن هذا تبديل جين واحد على الأقل مع تجنب تبديل تسلسل الجين بأكمله، يتم تبديل الجينات قبل نقطة التقاطع بين الوالد الأول (parent1) والوالد الثاني (parent2). يتم من خلال هذه العملية خلط المادة الوراثية للآباء المختارين، مما يؤدي إلى إنتاج ذرية جديدة تحمل خصائص من كلا الوالدين.

4-1-6 تطبيق الطفرة (Perform Mutation)

تقدم الطفرة التنوع في السكان عن طريق تغيير جينات الأفراد بشكل عشوائي. يساعد هذا الخوارزمية على استكشاف مناطق جديدة من مساحة الحل التي قد لا يمكن الوصول إليها من خلال التقاطع وحده. سنستخدم الطفرة من النوع (Bit Flip). تتكرر الطفرة على كل جين في قائمة جينات الفرد (في هذا النوع يتم قلب بعض البتات الموجودة في سلسلة البتات بشكل عشوائي). يحور الفرد عن طريق تقليب البتات بناء على معدل الطفرة (0.05)، إذا كان الجين 0، فإنه يصبح 1. حيث لكل بت لديه احتمال 5% للتقليب، وبعد الطفرة، يتم إعادة حساب لياقة الأفراد المتحولين لتعكس التغييرات في جيناتهم. وكخطوة أخيرة يتم تحديث السكان وتتوقف الخوارزمية بعد إكمال عدد محدد من التكرارات للتأكد من أن الخوارزمية تستكشف مساحة الحل بشكل كافي.

4-2 تقوية مفاتيح الحمض النووي (DNA Key Strengthening):

في هذا القسم سنبدأ بشرح مراحل السيناريو الثاني من المنهجية المقترحة، في هذه المرحلة سيتم استخدام المنهج الهجين للخوارزمية الجينية المعزز بالذكاء في تشفير الحمض النووي وبشكل خاص في تقوية مفاتيح تشفير DNA ذات اللياقة الضعيفة التي تم توليدها باستخدام مولدات عشوائية، لاستخدامها لاحقا في التشفير بدلا من التخلص منها، بشكل يحاكي التطور البيولوجي (إصلاح الحمض النووي) حيث أن تقوية المفاتيح بدلا من إعادة توليد مفاتيح جديدة تحافظ على التنوع وتقلل من الحسابات، جهد الحوسبة، الوقت المستغرق لتوليد المفاتيح، ويزيد من عشوائية هذه المفاتيح[7]. سيتم في هذه المرحلة اختيار وظائف اللياقة وتطبيق العوامل الوراثية وتعديلها لتناسب أساسيات تشفير DNA على عكس وظائف اللياقة لمخططات التشفير التقليدية. يبين الشكل (3) المنهج المتبع في تقوية مفاتيح DNA.



الشكل (3) منهجية تقوية مفاتيح التشفير القائمة على الحمض النووي

4-2-1 توليد المجتمع الأولي (Generate initial key population)

في تشفير الحمض النووي سيتم تمثيل أفراد المجتمع على شكل تسلسلات عشوائية مكونة من نيوكليوتيدات الحمض النووي والتي يتم تمثيلها بالأحرف "A"و "T"و "C"و "G". وهذه النيوكليوتيدات هي اللبنات الأساسية لتتابعات الحمض النووي. تتمثل المهمة الأساسية الأولى هنا في اختيار القيم المناسبة ل N و M لتوليد السكان الأوليين M × N من خلال مولد مفتاح حمض نووي عشوائي حيث M : هو طول كل سلسلة من سلاسل الحمض النووي و N هو عدد سلاسل الحمض النووي (DNA).

4-2-2 تحديد وظائف اللياقة (Define the fitness function)

تم تقييم تسلسلات المجتمع الأولي للمفاتيح باستخدام اختبارين للياق [7] : اختبار التردد (frequency Test) للتحقق من توزيع متوازن للنيوكليوتيدات (A, T, C, G) بحيث يقارب كل منها 25% من طول المفتاح، واختبار الفجوة (Gap Test) لتحديد عدد التكرارات المتتالية، حيث يُسمح بثلاث تكرارات كحد أقصى. تُصنَّف

المفاتيح التي تجتاز الاختبارين كقوية وتُستخدم مباشرة في التشفير، بينما تُعالج المفاتيح الضعيفة بالمنهجية الهجينة المقترحة لتعزيز قوتها.

4-2-3 تحديد وظائف اللياقة للمفاتيح الضعيفة (Defining Fitness Functions for Weak Keys)

بداية يتم تحديد وظيفتي اللياقة λ1 و λ2 بناء على اختبار التردد واختبار الفجوة، على التوالي. ويتم بعدها حساب λ عن طريق جمع القيم التي يتم الحصول عليها من λ1 وλ2. وأخيرا، يتم حساب وظيفة اللياقة البدنية F. لحساب λ1 ، دع العدد الإجمالي للمفاتيح الضعيفة يكون n، يتم تخزين تكرار أو عدد تكرارات A و T و C و G في أربعة متغيرات A و T و C و G على التوالي. يتم تخزين القيمة المثالية للتردد والتي تبلغ حوالي 25% من طول المفاتيح في المتغير i. بعد ذلك، يتم تطبيق مفهوم الانحراف المعياري لإيجاد انحراف التردد الذي تم الحصول عليه عن التردد المثالي لكل من النيوكليوتيدات الأربعة وتخزينها في σA و σT و σC و σG. أخيرا، يتم حساب λ1 كمتوسط σA و σT و σC و σG .

تعطي المعادلات (4,9) الصيغ اللازمة لحساب $\boldsymbol{\lambda}$ [7] :

$$\boldsymbol{\sigma_A = \sqrt{\frac{(i-a)^2}{n}}} \quad (4)$$

$$\boldsymbol{\sigma_T = \sqrt{\frac{(i-t)^2}{n}}} \quad (5)$$

$$\boldsymbol{\sigma_C = \sqrt{\frac{(i-c)^2}{n}}} \quad (6)$$

$$\boldsymbol{\sigma_G = \sqrt{\frac{(i-g)^2}{n}}} \quad (7)$$

$$\boldsymbol{\lambda_1 = (\sigma_A+\sigma_T+\sigma_C+\sigma_G)/4} \quad (8)$$

يتم بعدها حساب λ2 لإظهار سلسلة الحمض النووي التي تحتوي على أكثر من ثلاثة تكرارات متكررة لأي من النيوكليوتيدات الأربعة. يتم فحص كل مفتاح من المفاتيح الضعيفة الناتجة. إذا تم الحصول على مثل هذا السيناريو لأي من A أو T أو C أو G ، تكون λ2 =1 وإلا 0. يتم حساب قيمة λ عن طريق جمع القيم الفردية ل λ1 و λ2 كما هو موضح في المعادلة (9).

$$\boldsymbol{\lambda = \lambda_1 + \lambda_2} \quad (9)$$

بعد حساب λ لكل مفتاح من المفاتيح الضعيفة. يتم حساب دالة اللياقة النهائية F المعبر عنها وفق الصيغة (10) التالية [7]:

$$\boldsymbol{F = \frac{1}{1+e^{\lambda}}} \quad (10)$$

قيمة أعلى = لياقة أفضل (القيمة الأقرب ل1) وتعبر قيمة اللياقة (1) درجة مثالية أي توزع مثالي للنيكليوتيدات وبدون تكرار، والدرجة (0) هي أسوأ نتيجة ومعناها اختلال شديد في التوازن أو التوزيع بالإضافة أنها تحوي تكرار. تعتبر المفاتيح التي تعمل بشكل جيد في اختبار التردد واختبار الفجوة أكثر ملاءمة مقارنة بنظيراتها الأخرى. وبالتالي، فإن القيمة الأقل ل λ تعني قيمة أفضل ل F.

4-2-4 ترتيب وظيفة اللياقة للمفاتيح تنازليا (Sorting the Fitness Function Values of the Keys in Descending Order)

بعد حساب دالة اللياقة F، يتم ترتيب المفاتيح الضعيفة بترتيب تنازلي لقيم لياقتهم ببساطة عن طريق مقارنة القيم وفرزها. على الرغم من أن الخطوة بسيطة، إلا أنها تحمل أهمية كبيرة، حيث سيتم اختيار المفاتيح الأصلح لتقويتها في المراحل اللاحقة لاستخدامها في التشفير وهو الهدف من المنهج المقترح.

5-2-4 تحديث السرعة (Velocity Update)

سيتم تعديل سرعات الأفراد (المفاتيح) لتوجيه حركتهم في مساحة الحل باستخدام النهج القائم على الذكاء حيث سيتم اختيار الفردين الأكثر لياقة من قائمة المفاتيح الضعيفة المرتبة تنازليا. ويتم إضافة المزيد من العشوائية للفردين المختارين من خلال توليد بت عشوائي، حيث يُدخل هذا البت العشوائي عشوائية محكومة مما يشجع على الاستكشاف العشوائي بشكل يحاكي الذكاء الطبيعي. هذا البت العشوائي هو رقم عشوائي بين (0,1)، سيتم إضافته لكل عنصر من عناصر متجه السرعة الخاص بالفردين المختارين أو تسلسلي الحمض النووي المختارين، ويتم بذلك تحديث سرعة هذين الفردين. يمكن التعبير عن تحديث السرعة (الاستكشاف المستمر) بالعلاقة (11) التالية:

$$V_P^{i+1}[J]=V_P^T[J]+r_p[j] \quad (11)$$

حيث:

- $V_P^T[J]$: سرعة التسلسل P في موضع الجين j عند التكرار t.
- $r_p[j]\sim U(0,1)$، توزيع (بت) عشوائي موحد.

هذه المرحلة ضرورية لتحقيق التوازن بين الاستكشاف (العشوائية) والاستغلال في عملية التحسين، حيث تطور السرعات يسمح بالاستكشاف السلس لمساحة التسلسل.

6-2-4 تحديث الموضع (Position Update)

تقوم بتحديث مواقع الفردين المختارين من المجتمع بناءً على السرعات المحسوبة في الخطوة السابقة، حيث تترجم تحديثات السرعة تلك إلى تعديلات فعلية لتسلسل الحمض النووي مع الحفاظ على القيود البيولوجية. يتم تحويل السرعات المستمرة إلى تغيرات منفصلة في النيوكليوتيدات. مع ضمان بقاء جميع القيم ضمن [0,3] من خلال معالجة الفائض. أي يتم تطبيق السرعة الجديدة (المستمرة) على الموضع الحالي للفرد (الجينات) لتحريكه في اتجاه جديد. بمعنى آخر تتألف هذه المرحلة من خطوتين:

الخطوة الأولى: نضيف السرعة (المستمرة) إلى النيوكليوتيدات الحالية (المنفصلة)

الخطوة الثانية: التقريب إلى أقرب عدد صحيح والالتفاف عبر 4% للبقاء ضمن النطاق [0,3].

يمكن التعبير عن تحديث الموضع بالعلاقة(12) التالية:

$$x_p^{t+1}[j] = \square(nucl-to-num(x_p^t[j]) + v_p^{t+1}[j]) \quad (12)$$

حيث :

$x_p^{t+1}[j]\epsilon$[A,T,C,G]: الموضع الحالي للنيكليوتيدات .

nucl_to_num(·): يعين النيوكليوتيدات إلى{0,1,2,3}.

Q(): تابع التكمية التي يفرض قواعد الحمض النووي:

$$Q(z)=\text{num\_to\_nucl}((\text{round}(z)) \bmod 4) \quad (13)$$

4-2-7 إجراء التقاطع (Perform Crossover)

بعد تحديث سرعة وموضع تسلسل الحمض النووي للفردين الضعيفين ذو اللياقة الأعلى ستكون المهمة التالية هي اختيار نوع عملية التقاطع التي سيتم اجراؤها على هذين الوالدين أو تسلسلي الحمض النووي(parents)، في هذا المنهج المقترح، نركز على التقاطع بنقطة واحدة، لتحقيق تقاطع متوازن إلى حد ما، وتم اعتماد نقطة التقاطع في المنتصف، حيث أن آلية التقاطع لكل زوج من الأفراد تتم وفق التالي:

- النصف الأول من الوالد1 والنصف الثاني من الوالد 2 يعطي Child1
- النصف الأول من الوالد 2 والنصف الثاني من الوالد 1 يعطي Child2
- إذا لم يكن لأحد سلاسل الأب زوج، يتم تركها كما هي.

4-2-8 إجراء الطفرة (Perform Mutation)

يعتمد البحث على تطبيق الطفرة [7] بهدف تحقيق توزيع أكثر توازناً للنيوكليوتيدات في مفاتيح DNA الناتجة بعد التقاطع، مما يعزز ملاءمتها للتشفير. تتم العملية عبر تحديد القاعدة الأقل والأكثر تكراراً واستبدال جزء من الأكثر تكراراً بالأقل، مع مراعاة ألا يتجاوز التكرار ثلاث مرات متتالية لضمان اجتياز اختبار الفجوة. بعد ذلك يُعاد تقييم المفاتيح وتطبيق خطوات التحسين (تحديث السرعة والموضع، التقاطع والطفرة) بشكل متكرر حتى تُصنَّف جميع المفاتيح كقوية وصالحة للاستخدام في التشفير. في حال وجود أكثر من قاعدة لها نفس القيمة الدنيا (Min)، يتم اختيار واحدة فقط. وإذا كان هناك أكثر من قاعدة لها نفس القيمة العليا (Max)، يتم اختيار القاعدة التي تحتوي على أكبر عدد من التكرارات المتتالية، لأن هذا يجعل المفتاح أكثر تأهيلاً لاجتياز اختبار الفجوة (Gap Test) في المستقبل. لنفترض أن m هو عدد مرات حدوث القاعدة النيتروجينية المراد تحويرها. يتم حساب m باستخدام المعادلة[7]:

$$m = i - \text{Min}(a, t, c, g) \quad (14)$$

5- النتائج والمناقشة (Results and Discussion)

بعد تحديد المنهجية المقترحة ووصف خطواتها التفصيلية، يعرض القسم التالي النتائج العملية المستخلصة من تطبيق النموذج، مع تحليل أدائه. سيتم في هذا القسم مناقشة نتائج كل سيناريو بشكل منفصل. تم تنفيذ المنهجية المقترحة بلغة Python وتقييم أداء المفاتيح الناتجة باستخدام مقاييس العشوائية والتفرد والأمان، مع اعتماد متوسط القيم لتجاوز التباين الناتج عن ظروف التشغيل. يعتمد النموذج على مزيج من التحسين المحلي والاستكشاف العشوائي لتحقيق توازن بين الكفاءة الحسابية وجودة المفاتيح. وقد أثبتت النتائج في كلا السيناريوهين فعالية عالية في تحسين المفاتيح وتقويتها، مع تقليل الجهد الحسابي وتعزيز مقاومتها للهجمات الأمنية، وسيتم تحليل كل سيناريو على حدة.

5-1 نتائج السيناريو الأول: مرحلة توليد المفاتيح الثنائية (Binary Key Generation System)

في هذا الجزء، تم توليد مفاتيح ثنائية بحجم 64 بت، باستخدام الخوارزمية الجينية المعززة بالذكاء المحلي، وتقييمها باستخدام ثلاثة مقاييس أداء (Performance Metrics):

- **Shannon Entropy**
- **Hamming Distance**
- **Correlation Coefficient**

بعد تنفيذ المرحلة الأولى، يتم تحليل النتائج وللقيام بذلك بداية سنحدد قيم المعلمات التالية:

حجم المفتاح 64bit.

عدد الأجيال 1000.

نوع الاختيار: عجلة روليت.

نوع التقاطع: نقطة واحدة Single-Point Crossover ، معدل التقاطع :0.7.

نوع الطفرة: bit flip، معدل الطفرة : 0.05 .

5-1-1 مقاييس الأداء(Performance Metrics)

انتروبيا شانون: لمعرفة مدى عشوائية المفاتيح المولدة أو تنوع توزع جينات الأفراد (توزع القيم الثنائية في المفاتيح المولدة)، قمنا بحساب وظيفة الانتروبيا لجينات السكان لدينا، حيث يمكن استخدام الانتروبيا في الخوارزميات التطورية أو الخوارزميات الجينية أو طرق التحسين العشوائي الأخرى لقياس التنوع السكاني، تشير الانتروبيا الأعلى أن السكان متنوعون ولا يتقاربون بسرعة كبيرة [8] . صيغة أنتروبيا شانون (Shannon Entropy):

$$H = -(P(0)LOG_2(P(0)) + P(1)LOG_2(P(1)) \quad (15)$$

عند قياس انتروبيا شانون لعدد أجيال 1000 وحجم مفتاح 64 أعطت الخوارزمية الهجينة المقترحة أن درجة عشوائية المفاتيح المتولدة هي1 كما هو في الشكل (4).

```
Key Size: 64
Population Size: 64
Number of Generations: 36
Time taken: 0.016980409622192383 seconds
Degree of Randomness (Entropy): 1.0
```

الشكل (4): قياس درجة العشوائية للمفاتيح المولدة

مسافة هامينج (Hamming Distance): هي مقياس للفرق بين سلسلتين ثنائيتين (أو تسلسلين متساويين في الطول). يتم حسابها على أنها عدد المواضع التي تختلف فيها البتات المقابلة[9]. التعريف الرياضي: بالنظر إلى سلسلتين ثنائيتين X و Yبطول n، فإن مسافة هامينج H(X, Y) تُعرف على النحو التالي :

$$H(X.Y) = \sum_{i=1}^{n}(X_i \neq Y_i) \quad (16)$$

حيث:

X_i و Y_i هما البتات في الموضع i،

≠ تمثل عدم التطابق

عند تنفيذ المنهجية المقترحة لمفاتيح ثنائية حجمها 64 بت كان متوسط مسافة هامينغ بين المفاتيح المولدة32.0267 . كما هو موضح بالشكل(5).

```
Average Hamming Distance: 32.026785714285715
```

الشكل(5) : متوسط مسافة هامينغ للمفاتيح

قياس معامل الارتباط (Correlation Coefficient): يقيس معامل الارتباط العلاقة بين مجموعتين من البيانات. يقوم بتقييم التشابه بين مفتاحين تم إنشاؤهما من خلال تحديد كيفية ارتباط البتات الخاصة بهما.

التعريف الرياضي المعبر عنه في الصيغة التالية [10]:

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - X)^2 (Y_i - Y)^2}} \quad (17)$$

حيث:

X ,Y هما قيم المفتاحين،

$\bar{Y}$ و $\bar{X}$ هي قيمهم المتوسطة

r معامل الارتباط النسبي و مجال القيم له من 1−الى 1:

r =1 (المفاتيح متشابهة جدا)

r =0 (لا يوجد ارتباط أي عشوائي تماما)

r =1− (ارتباط سلبي مثالي)

عند تنفيذ المنهجية المقترحة كانت نتيجة متوسط معامل الارتباط بين المفاتيح هي (0.0005−)، كما هو موضح في الشكل (6).

```
Average Hamming Distance: 32.026785714285715
Average Correlation Coefficient: -0.000558892154040716
Key Size: 64
Population Size: 64
```

الشكل (6): معامل الارتباط للمفاتيح

5−1−2 مناقشة نتائج السيناريو الأول:

يمكن أن يكون استخدام المنهج القائم على الذكاء المحلي أو الخوارزمية الجينية فعالاً بمفرده، لكن المنهج الهجين الذي يعزز الخوارزمية الجينية بالذكاء يحقق أفضل النتائج في توليد مفاتيح تشفير ثنائية عشوائية، موازنًا بين التنوع والاستقلالية. الجدول التالي: يعرض ملخص تحليل عشوائية وتفرد مفاتيح التشفير المتولدة حسب المقاييس المعتمدة في بحثنا.

Metric	Value	Ideal Range
Entropy	1.0	[0.9-1.0]
Avg. Hamming Distance	32.0267	[28-32]
Correlation	-0.000558	[-0.1,0.1]

يظهر الجدول التالي أن قيمة الانتروبيا بلغت 1، مما يشير إلى عشوائية مثالية للمفاتيح وضمان مقاومتها لهجمات القوة الغاشمة. متوسط مسافة هامينغ الناتج هو 32.0267 لمفاتيح بطول 64 بت، ما يعكس تفردًا عاليًا ويقارب القيمة النظرية المتوقعة 32، مما يصعب التنبؤ بالمفاتيح أو تخمينها. كما بلغ معامل الارتباط – 0.000558، قريبًا من الصفر المثالي، دالاً على استقلالية المفاتيح وعدم وجود علاقة خطية بينها، وهو عامل أساسي لمقاومة الهجمات التحليلية.

5-2 نتائج السيناريو الثاني: مرحلة تقوية مفاتيح تشفير الحمض النووي (DNA-Based Key Strengthening)

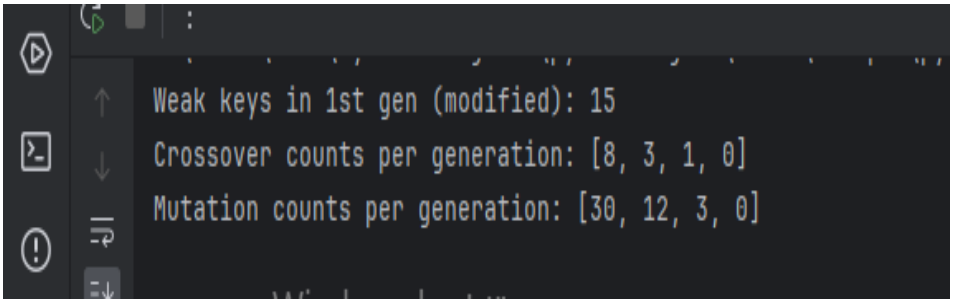
سيتم تحليل نتائج السيناريو الثاني لتحقق من قدرة المنهج المقترح على تقوية مفاتيح تشفير DNA الضعيفة من خلال تتبع عدد عمليات التقاطع والطفرة التي سيتم استخدامها لتعزيز المفاتيح الضعيفة وذلك لدورها في قياس مدى قوة الخوارزمية في استكشاف مساحة الحل، بداية سنقوم بتحديد البارامترات التي سيتم تنفيذ الخوارزمية عندها:

- حجم مفتاح DNA: 25
- المجموعة الأولية للسكان: 25*25.
- عدد الأجيال: 20 جيل
- سيتم تمثيل نيوكليوتيدات الحمض النووي [A=0 ,T=1,C=2,G=3]

في هذه المرحلة، تم توليد مجتمع أولي مكون من 625 مفتاحا (25*25) متمثلة بتسلسلات نيوكليوتيدية، وتم تصنيف 15 مفتاحا منها كمفاتيح ضعيفة بناء على اختباري التردد والفجوة.

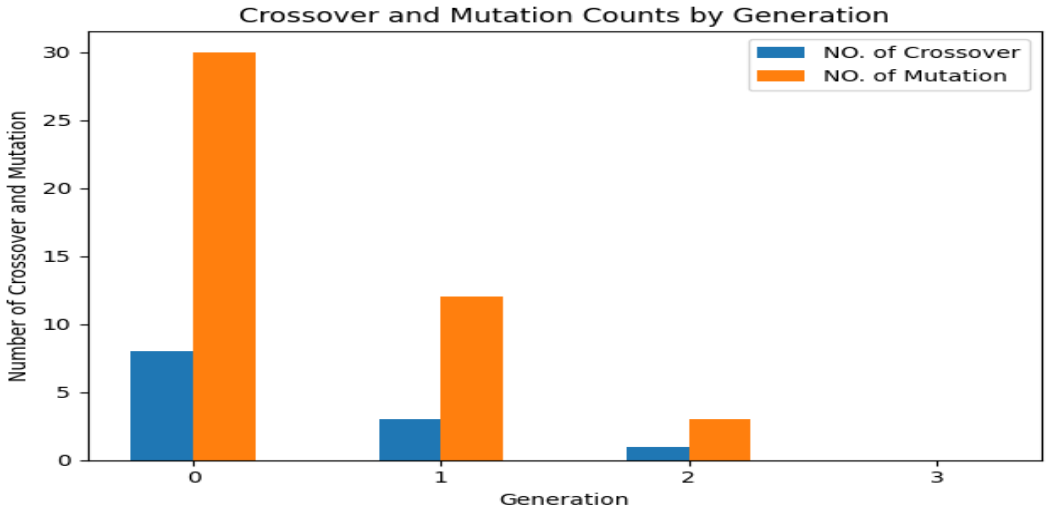
5-2-1 تحسين المفاتيح الضعيفة

من خلال تطبيق المنهج الهجين، تم تقوية جميع المفاتيح الضعيفة خلال 3 أجيال فقط، دون الحاجة إلى تعزيز إضافي. أظهرت الخوارزمية قدرة عالية على استكشاف مساحة الحل وتصحيح الانحرافات البيولوجية في التوزيع والتكرار.



الشكل (7): عدد المفاتيح الضعيفة للجيل الأول

5-2-2عدد عمليات التقاطع والطفرة:



الشكل (8): عدد عمليات التقاطع والطفرة لكل جيل

يعد تتبع عدد عمليات التقاطع والطفرات لكل جيل أمرا بالغ الأهمية، حيث يقيس مدى قوة الخوارزمية في استكشاف (التقاطع) وتصحيح (طفرة) مساحة الحل. يضمن التقاطع التنوع من خلال إعادة تجميع المادة الجينية من الأفراد الضعفاء ذوي اللياقة البدنية العالية، وتفرض الطفرة القيود البيولوجية حيث توازن النيوكليوتيدات ويزيل التكرارات مثلا AAAA. يعني معدل التقاطع والطفرة المرتفع أن معظم سلاسل الأطفال (child) مصنوعة من عمليات التقاطع والطفرات وهذا يعني أنه يعزز التنوع الجيني ويمنع التقارب المبكر ومع ذلك ، يؤثر هذا سلبا على تعقيد وقت تشغيل النظام.

بالنسبة لعدد عمليات التقاطع: ينخفض على مر الأجيال مع تقارب السكان نحو تسلسلات أكثر لياقة (عدد أقل من الأفراد "الضعفاء" المؤهلين للتقاطع). وتشير معدلات التقاطع الأولية المرتفعة إلى استكشاف حلول متنوعة في وقت مبكر(أي تعزز النوع الجيني) ومنع التقارب المبكر، بينما تشير المعدلات المنخفضة اللاحقة إلى الاستقرار اي تقارب السكان نحو تسلسلات أكثر لياقة .

أما بالنسبة لعدد عمليات الطفرة: تصل معدلات الطفرة ذروتها في بداية المحاكاة ثم تنخفض حيث تقوم الخوارزمية بتصحيح الانحرافات بنشاط، ثم تنخفض مع اقتراب التسلسلات من التوازن أي التسلسلات أصبحت جميعها تفي القيود. بشكل عام يبين المخطط أنه مع كل مجموعة سكانية جديدة، يتناقص عدد العمليات الجينية التي سيتم تطبيقها بشكل كبير مما يقلل من تعقيد النظام. ويوضح تقاربا فعالا نحو تسلسلات الحمض النووي المعقولة بيولوجيا، مع عدد التقاطع والطفرات التي تعكس توازنا بين الاستكشاف والاستغلال.

6- الاستنتاجات والتوصيات (Conclusions and Recommendations)

استنادا إلى ما تم عرضه من نتائج ومناقشة يمكن تلخيص الإسهامات الأساسية لهذا المقال. حبث ساهم هذا النهج الهجين في تحقيق توازن مثالي بين الاستكشاف العشوائي الواسع والاستغلال الموجه للحلول ذات اللياقة العالية، ما انعكس إيجابًا على جودة المفاتيح الناتجة من حيث العشوائية، التفرد، والقدرة على مقاومة الهجمات. تم إجراء البحث بالاعتماد على بارامترات مشابهة لتلك المستخدمة في الدراسات المرجعية[1,13] التي تم الاعتماد عليها في هذا البحث وذلك بهدف القيام بمقارنات صحيحة. أبرز الاستنتاجات التي توصلنا إليها:

A. تحقيق عشوائية مثالية: حيث بلغت المفاتيح الثنائية المولدة باستخدام المنهج الهجين أعلى درجات الانتروبيا (1.0)، ما يدل على أقصى درجات العشوائية المطلوبة لتأمين البيانات ضد هجمات التنبؤ والتحليل الإحصائي.

B. تفرد واستقلالية المفاتيح: أظهرت المفاتيح متوسط مسافة هامينغ يقارب 32 (للمفاتيح ذات الطول 64-بت)، ومعامل ارتباط قريب من الصفر (0.0005-)، ما يؤكد استقلالها الإحصائي وتفردها البنيوي.

C. تحسين مفاتيح DNA الضعيفة: استطاع المنهج الهجين تقوية جميع المفاتيح الضعيفة ضمن عدد محدود من الأجيال، دون الحاجة إلى تعزيز إضافي، مما يوفّر الجهد الحوسبي ويزيد من كفاءة التشفير البيولوجي.

D. الحصانة الأمنية: تعزز المفاتيح المستندة إلى الحمض النووي مساحة البحث التشفيري إلى قوة أسية أعلى بمقدار 8 مرات من المفاتيح الثنائية، ما يجعلها محصنة عمليًا ضد هجمات القوة الغاشمة.

يقترح البحث التعديلات والتطويرات التالية التي تضيف أفكارا جديدة في مجال تحسين دور الخوارزمية الجينية في توليد المفاتيح لاستخدامها في مختلف تطبيقات التشفير:

1- يمكن أن تركز الأعمال المستقبلية على تطوير إطار عمل برمجي مفتوح المصدر لتوليد المفاتيح باستخدام الخوارزمية الجينية المدعومة بالذكاء المحلي، بحيث يمكن للمجتمع البحثي تجربته وتطويره.

2- كما يمكن يجب تقييم المنهج المقترح ضد هجمات تحليلية متقدمة مثل هجمات التوقيت(Timing Attacks) أو هجمات التفريق(Differential Attacks) ، وذلك للتحقق من المتانة الواقعية للمنظومة.

المراجع

[1] H. Singh, A. Gupta, and R. S. Rana, “DNA-PRESENT: A DNA-Inspired Lightweight Encryption Algorithm for Low-Powered IoT Devices,” Sensors, vol. 24, no. 24, p. 7900, Dec. 2024.

[2] S. Sharma and A. Kumar, “An Optimized Genetic Algorithm-Based Non-Commutative Encryption for Cloud Data Security,” International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 12, no. 4, pp. 25–33, 2024.

[3] P. Mukherjee, C. Pradhan, and G. Srivastava, “A GA–GAN Approach for Next-Generation Cryptographic Security,” Information Retrieval Journal, Springer, vol. 28, pp. 553–570, Jan. 2025.

[4] M. J. Arshad, M. Umair, S. Munawar, N. Naveed, and H. Naeem, "Improving cloud data encryption using customized genetic algorithm," *International Journal of Intelligent Systems and Applications*, vol. 12, no. 6, pp. 28–36, Dec. 2020.

[5] A. H. S. Alves, G. A. C. Neto, M. S. Gomes, L. D. Santos, P. L. L. Bertarini, and L. R. do Amaral, "Binary or integer chromosome: Which is the best structure for supervised machine learning using genetic algorithms," *Applied Sciences*, vol. 15, no. 5, p. 2608, Mar. 2025.

[6] F. Li, X. Zhang, and Y. Wang, "The role of genetic algorithm selection operators in extending WSN stability period: A comparative study," *Electronics*, vol. 11, no. 1, Art. 28, Jan. 2022.

[7] P. Mukherjee, H. Garg, C. Pradhan, S. Ghosh, S. Chowdhury, and G. Srivastava, "Best fit DNA-based cryptographic keys: The genetic algorithm approach," *Sensors*, vol. 22, no. 19, p. 7332, 2022.

[8] K. Silva, P. Serpa, D. Sgrott, F. Miranda, F. Cerqueira, J. S. Filho, and R. S. Parpinelli, "Diversity-guided multi-objective evolutionary algorithm applied to steel development," in *Hybrid Intelligent Systems*, Lecture Notes in Networks and Systems, vol. 1226, pp. 133–142, 2025.

[9] T. Lässig, B. Doerr, N. Hansen, and C. Witt, “Analysing Equilibrium States for Population Diversity,” *Algorithmica*, vol. 86, pp. 3245–3275, 2024.

[10] M. Harary, Efficient algorithms for the sensitivities of the Pearson correlation coefficient and its statistical significance to online data, *arXiv preprint* arXiv:2405.14686, rev. Jun 9, 2024.