مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١٠) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (10) 2025

استخدام العلامات الحيوية في توليد مفاتيح التشفير في شبكات حساسات الجسم اللاسلكية

د. بشرى معلا•

م. خديجة اسكندر ••

(تاريخ الإيداع ٢٠٢٥/٦/٣ . قُبِل للنشر في ٢٠٢٥/٨/٢٥)

□ ملخّص □

يعدّ استخدام العلامات الحيوية من أكثر الطرائق الفعالة في حماية الاتصالات ضمن شبكات حساسات الجسم اللاسلكية Wireless Body Sensor Networks (WBSNs)، إذ يُستخدم جسم المريض نفسه كوسيلة لتوليد مفاتيح تعمية من خلال العلامات الحيوية ويطلق عليها اسم المفاتيح البيومترية. ورغم أن استخدام العلامات الحيوية التقليدية قد رفع مستوى الأمن ضمن أنظمة الحماية إلا أنه يعاني من عدة سلبيات، مما دفع إلى التوجه إلى علامات حيوية جديدة أكثر فعالية مثل حساسات تخطيط كهربائية القلب ElectroCardioGram (ECG) ، وحساس تخطيط الدماغ ElectroEncephaloGraphy (EEG) .

سنقدم في بحثنا هذا مخططاً لتوليد سلاسل أرقام عشوائية طول كل منها ١٠٢٤ بت بالاعتماد على دمج كل من مميزات إشارة تخطيط القلب ECG، و مميزات إشارات تخطيط الدماغ الخاصة بتخيل الحركة ، درسنا عشوائية هذه السلاسل من خلال الاختبارات الإحصائية للمعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology (NIST)، كما درسنا خاصية التميز (التفرد) لهذه السلاسل من خلال مسافة هامينغ، وتبين لنا إمكانية استخدام هذه السلاسل كمفاتيح تشفير في شبكات WBSNs.

كلمات مفتاحية : توليد أرقام عشوائية، العلامات الحيوية، حساس تخطيط كهربائية القلب (ECG) ، حساس تخطيط كهربائية الدماغ (EEG)، تخيل الحركة، NIST .

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
boushra.maala@gmail.com
•• طالبة دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
khadijeh.iskander@tishreen.edu.sy

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١٠) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (10) 2025

Using of Biometrics in Generation Encryption keys at Wireless Body Sensor Networks

Dr. Boushra Maala*
Eng. Khadijeh Iskander**

(Received 3/6/2025 . Accepted 25/8/2025)

□ ABSTRACT □

Using biometric parameters is very effective way to protect communication over Wireless Body Sensor Networks (WBSNs). We can use patient body to generate cryptography keys by biometric parameters, and we call them biometric keys. Even that using traditional biometric parameters increases security degree in protection systems, it has many disadvantages, which encouraged using more effective biometric parameters such as Electrocardiograms (ECG) and ElectroEncephaloGraphy(EEG).

In this paper, we present a scheme for generating 1024-bit random number strings by combining both ECG signal features using the MIT_BIH Arrhythmia database, and EEG signal features for motion imagery using the EEG Motor Movement/Imagery. We studied the randomness of these strings through National Institute of Standards and Technology (NIST) statistical tests, studied the distinctiveness of these strings through the Hamming distance, and showed that these strings can be used as encryption keys in security applications.

Key words: random number generation, biometrics, ElectroEncephaloGraphy(EEG), ElectroCardioGram (ECG), Movement Imagery (MI).

* Assistant Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. boushra.maala@gmail.com
** PhD Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. khadijeh.iskander@tishreen.edu.sy

مقدمة:

تُعدّ شبكات حساسات الجسم اللاسلكية Wireless Body Sensor Networks (WBSNs) تقنية للمراقبة المستمرة عن بُعد للنشاط الفيزيولوجي والسلوكي لجسم الإنسان فتلعب بذلك دوراً كبيراً في تأمين الرعاية الصحية عن بعد. إذ تتألف هذه الشبكة من عقد حساسة صغيرة الحجم، ذاتية التغذية ومحدودة الموارد قابلة للزرع بشكل دائم أو شبه دائم داخل جسم المريض أو تتوضع على سطح الجلد لأغراض طبية محددة، إذ تتحسس بارامترات معينة من جسم المريض تسمى العلامات الحيوية. و لقد أثبتت شبكات WBSN أنها أساس مهم في منظومة العناية الصحية، لذا فإن استخدامها يلحظ انتشاراً واسعاً في السنوات الأخيرة، ونظراً لحساسية البيانات المنقولة عبر الشبكة و المتعلقة بالحالة الصحية للمريض فإن قضايا الأمن والخصوصية تُعدّ أمراً مهماً للدراسة، إذ أنّ أي تسريب أو تلاعب في سجلات المريض قد تودي بحياته، ومن الممكن استغلال هذه السجلات لأغراض أخرى [1].

اقترحت العديد من تقنيات الحماية لضمان متطلبات الأمن في هذه الشبكات، وتعدّ عملية توليد مفاتيح تعمية آمنة وتوزيعها وحمايتها أمراً مهمّاً لضمان فعالية هذه التقنيات. استخدمت العلامات الحيوية التي تعدّ من أكثر الوسائل الأمنية فعالية في هذه الشبكات، إذ تستخدم خصائص جسم المريض كوسيلة لتوليد مفاتيح وبصمات حيوية خاصة بهذا المريض [2]. رغم أن استخدام العلامات الحيوية مثل بصمة الإصبع أو الوجه أو الصوت وخط اليد قد رفع مستوى الأمن ضمن أنظمة الحماية، ولكن المعلومات التي تحملها هذه العلامات الحيوية هي موروثة وفريدة ولا يمكن تغييرها من أجل استخدامها مع تطبيقات مختلفة، لذا في حال سُرقت العلامة الحيوية المستخدمة فإن جميع المفاتيح السرية المولدة عن طريقها عرضة للكسر. كما يرافق العلامات الحيوية سابقة الذكر ضجيج بشكل طبيعي مما يفرض قيوداً فيما يتعلق بالتقنية المطلوبة لقراءة العلامة الحيوية. إضافة إلى أن ضمان أمن أي نظام يتطلب تغيير مفاتيح التعمية كل فترة زمنية معينة. وبما أن العلامات الحيوية التقليدية موروثة وغير قابلة للتغيير فإن المفاتيح المولدة من خلالها أيضاً ذات فضاء محدود وهذا يُعدّ مشكلة عند استخدامها في تأمين حساب بنكي أو بريد الكتروني، وهذا ما أشرنا إليه سابقاً في أن سرقة العلامة الحيوية تؤدي لتعريض جميع التطبيقات المؤمنة من خلالها لخطر الاختراق.

اعتُمِد في كثير من الأنظمة المتقدمة على بصمة الإصبع والقزحية والوجه معاً لزيادة السوية الأمنية لها، إلا أنها قد تكون مكشوفة للعلن وغير سرية، بمعنى أن التقاط صورة للوجه أو تسجيل صوت المستخدم أو سرقة بصمة الأصابع يُعدّ أمراً ممكناً [3].

كل ما سبق دفع للتوجه لعلامات حيوية جديدة لا تمتلك نقاط الضعف الموجودة في العلامات الحيوية التقليدية، ونذكر منها إشارات حساسات تخطيط كهربائية القلب ElectroCardioGram (ECG)، وتخطيط كهربائية الدماغ ElectroEncephaloGraphy(EEG).

الدراسات المرجعية:

سنورد فيما يأتي العديد من الأبحاث حول استخدام مميزات إشارتي تخطيط القلب والدماغ في القضايا الأمنية:

اعتمدت العديد من الدراسات على إشارة تخطيط القلب الكهربائية في توليد أرقام عشوائية، استخدمت بعض هذه الدراسات قيم مطالات إشارة ECG كمميزات لأغراض أمنية [4]، ولكن هذه المطالات

لإشارتي ECG مقاستين بالتزامن من نقطتين مختلفتين من جسم الإنسان تكون متفاوتة بشكل ملحوظ وتعتمد بشكل أساس على المسافة من القلب. استخدمت دراسات أخرى قيم (Inter-Pulse-Intervals (IPI (وهي الفترة الزمنية الفاصلة بين قمتين متتاليتين متشابهتين) فقط لإشارة ECG ولكن هذه الدراسات تعاني من أداء منخفض، إذ أن الزمن الفاصل بين نبضتي قلب متتاليتين يمكن تحديده من خلال كاميرا أو تحليل لون الجلد وهذا يجعل الخوارزمية المعتمدة على هذه القيم فقط أقل أماناً [5, 6].

اعتمدت الدراسة [7] على قيم IPI، إذ أُخذت آخر أربع بتات فقط من كل قيمة IPI، فمن أجل توليد سلسلة بطول ١٢٨ بت كان هناك حاجة لـ ٣٣ ضربة قلب؛ أي زمن يتراوح ما بين ٢٠-٣٠ ثانية. أما الدراسة [8] اعتمدت على نبضة قلب واحدة واستخرجت منها جميع المميزات لإنتاج (١٦ بت)، وبالنتيجة كان هناك حاجة لـ ٨ نبضات قلب لإنتاج سلسلة بطول ١٢٨ بت وهذا يعد غير فعال من ناحية استهلاك الزمن.

أما بالنسبة لإشارة تخطيط الدماغ فقد دُرس النشاط الكهربائي للدماغ في عدة حالات:

١- **حالة الراحة:** حيث أن الشخص لا يمارس أي نشاط أو مهمة، وإنما يبقى هادئاً ومستيقظاً فقط. وبينت الدراسات أن النشاط الدماغي لأشخاص مختلفين وهم في حالة السكون أو الراحة يكون مختلفاً ومتمايزاً بين هؤلاء الأشخاص، وأن الخصائص التي يحملها هذا التسجيل تكون فريدة ومميزة. ولكن تطبيق هذه الحالة صعبة في العالم الخارجي الحقيقي، إذ أنه من الصعب تأمين حالة سكون تام للشخص.

في المرجع [9]، طبقت الدراسة على أشخاص أصحاء وأشخاص مرضى مصابين بالصرع في حالتين (أعين مفتوحة وأعين مغلقة) وهم في حالة سكون دون القيام بأي نشاط، واستخدمت ١٠٠ قناة و حصلت الترددات من القيم الصحيحة لإشارة EEG ومن ثم ولدت سلاسل بطول 10^6، ولكن بينت هذه الدراسة أنه لا يمكن استخدام إشارة EEG بشكل مباشر كمولد لسلاسل الأرقام العشوائية، وإنما يجب إخضاع هذه السلاسل لعميات تحويل رياضية لجعلها عشوائية.

في المرجع [10]، طورت الدراسة السابقة، وأُخذت قيم حقيقية وضربت بـ 10^m لتحويلها إلى قيم صحيحة ومن ثم أجريت إزاحة نحو اليمين، استخدم ٦٤ الكترود، وأنتجت سلاسل بطول 10^6، وبينت هذه الدراسة أن نطاق الترددي غاما(gamma) قد أعطى أفضل النتائج.

٢- **حالة الحركة:** يعني تسجيل النشاط الدماغي للفرد أثناء قيامه بأداء مهمة معينة أو إدراكه لفعل معين.

أو تسجيل النشاط الدماغي للفرد استجابة لتأثير بصري خارجي، مثل صورة مرئية أو فلاش.

اعتمدت الدراسة [11] على تسجيل النشاط الدماغي لـ ٧ أشخاص أثناء قيامهم بأداء ٥ مهام عقلية معينة، استخدمت ٦ قنوات، واستمر التسجيل الكهربائي لمدة ١٠ ثواني، ومن ثم أجريت المعالجة واستخراج المميزات باستخدام تحويلي ويفلت المتقطع و فوريه المتقطع، وبالنتيجة تم الحصول على مفاتيح بطول ٢٣٠ بت.

في الدراسة [12] أجريت عملية تحقق بيومتري من خلال تسجيل النشاط الدماغي للأشخاص وهم يقومون بالتوقيع على هواتفهم، حيث دمجت مميزات إشارة EEG والتي تم تحصيلها باستخدام تحويل فوريه المتقطع DFT مع مميزات التوقيع الديناميكي. واستخدمت استخدام ١٤ قناة.

في الدراسة [13] سُجل النشاط الدماغي للأفراد وهم يقومون بإدخال كلمات مرور معينة من خلال لوحة المفاتيح. استخدمت ٥ قنوات وتم الحصول على سلاسل أرقام عشوائية بطول ١٦٠ بت.

في الدراسة [14] سُجل النشاط الدماغي للأشخاص استجابة لتأثير بصري خارجي من خلال النظر إلى صورة فيها خطوط بيضاء وسوداء واعتمدوا على الالكترود Cz لتوليد رمز PIN لاستخدامه في أغراض التحقق والأمن.

٣- **<u>حالة تخيل الحركة:</u>** يُسجل النشاط الدماغي للفرد أثناء تخيله تحريك جزء معين من جسمه أو تخيله القيام بمهمة معينة، وبينت الدراسات أن التسجيل الدماغي هنا يمتلك خصائص فريدة ومميزة، وأن هذا النوع أقل عرضة للضجيج من حالة الحركة الفعلية، وهذا ما جعله مناسباً للاستخدام في عمليات التوثيق والتحقق. وهو قابل للتطبيق ومناسب لكل أنواع المرضى المختلفين عن بعضهم بالمقدرات الفيزيائية والبصرية.

في الدراسة [15] وُضِع مخطط أمني بيومتري من أجل عمليات التحقق والتوثيق يعتمد على إشارات تخطيط الدماغ الخاصة بتخيل حركة الأرجل والأذرع والتي جمعت بواسطة 17 الكترود، نفذت التجربة بالاعتماد على ٤٠ شخص، مستخدمين خوارزميات التعلم العميق.

أيضاً تمكنت الدراسة [16] من تحسين دقة التحقق البيومتري بالاعتماد على أربع مميزات من إشارات تخطيط الدماغ الخاصة بتخيل الحركة، والتي جمعت باستخدام ٣٦ الكترود. واستخدم مرشح تمرير حزمة Hz (30-8) خلال طور المعالجة البدائية، واستغرقت التجربة ١٠ ثواني.

كان هناك أيضاً العديد من الأبحاث حول استخدام إشارات تخطيط الدماغ EEG في توليد أرقام عشوائية يمكن استخدامها كمفاتيح تعمية نذكر منها:

الدراسة [17] اعتمدت على التسجيلات الكهربائية لـ ٣٢ شخص مختارة بشكل عشوائي من قاعدة البيانات GrazIIIa ، حيث استخدمت ٦٤ قناة، و استخرجت المميزات الترددية PSD(power spectral density) ، وباستخدام التكميم وُلِدت مفاتيح طول كل منها ٢٥٦ بت.

الدراسة [18] اعتمدت على الالتزام الضبابي (fuzzy commitment) في عملية استخراج المميزات من إشارة تخطيط الدماغ لـ ٤٢ شخص، و أُنتجت سلاسل بتات عشوائية بطول ٤٠٠ بت يمكن استخدامها كمفاتيح تعمية أو في أغراض التحقق.

نلاحظ من هذه الدراسات المرجعية السابقة فعالية إشارات تخطيط القلب ECG و الدماغ EEG في استخدامها كعلامات حيوية في توليد أرقام عشوائية وأغراض التحقق، ولكن بقي هناك نقاط ضعف تتمثل بتعقيدات النظام والإنتاجية المنخفضة، لذلك نسعى في بحثنا هذا إلى تطوير هذه الدراسات من خلال اقتراح مخطط جديد يجمع بين مميزات كل من إشارات تخطيط القلب ECG و الدماغ EEG وإجراء المعالجة الأولية المناسبة لتخفيض الضجيج المرافق لهذه الإشارات وذلك لتشكيل سلاسل أرقام عشوائية آخذين بالحسبان تخفيض تعقيد النظام وزيادة الإنتاجية.

أهمية البحث و أهدافه:

إن تطور شبكات WBSN ودورها الفعال والمهم في الرعاية الصحية والمراقبة الطبية عن بعد للمرضى والمسنين بالإضافة إلى تطبيقاتها العديدة، جعل هذا النوع من الشبكات قضية مهمة في الكثير من البلدان، ونظراً لحساسية المعلومات المرسلة عبر هذه الشبكة، والخطورة الناتجة عن اختراق هذه المعلومات

والتي قد تودي بحياة الإنسان في بعض الحالات، هذا بدوره جعل تحقيق متطلبات الأمن والعمل على توفير الحماية لهذا النوع من الشبكات أمراً هاماً. يهدف بحثنا هذا إلى وضع مخطط أمني يشمل توليد مفاتيح تعمية آمنة وفعالة بالاعتماد على إشارات فيزيولوجية مقاسة من جسم المريض.

طرائق البحث و مواده:

تم تحصيل إشارة تخطيط القلب الكهربائية من قاعدة البيانات MIT-BIH Arrhythmia المضمنة في PhysioBank التي تعدّ من أشهر قواعد البيانات المستخدمة لأغراض التصنيف ودراسة القضايا الأمنية المتعلقة بالعلامات الحيوية. تتضمن قاعدة البيانات هذه العديد من تسجيلات إشارة ECG لأشخاص من الجنسين تتراوح أعمارهم من ٢٣ وحتى ٨٩ سنة، مدة كل منها ٣٠ دقيقة، وتردد أخذ العينات هو ٣٦٠عينة في الثانية [19].

اعتمدت هذه الدراسة على قاعدة البيانات waveform (WFDB) وهي عبارة عن حزمة برمجية تتضمن العديد من النماذج التي تتعامل مع إشارة تخطيط القلب الكهربائية من خلال قراءتها وتحليل بارامتراتها [20].

بينما تم تحصيل إشارة تخطيط الدماغ الكهربائية من قاعدة البيانات EEG Motor Movement/Imagery Dataset V1.0.0 المضمنة في PhysioBank أيضاً، اعتمدنا في دراستنا على المكتبة البرمجية (mne) والتي تتضمن العديد من النماذج التي تتعامل مع إشارة تخطيط الدماغ الكهربائية من خلال قراءتها وتحليل بارامتراتها [21].

وبرمجت جميع خطوات المخطط المقترح هنا باستخدام لغة الـ Python الإصدار 3.10 [22].

ونفذت على جهاز حاسب ذو مواصفات مبينة في الجدول الآتي :

الجدول (١) : بعض مواصفات الجهاز الذي طبقت عليه الدراسة.

نظام التشغيل Operating system	المعالج Processor	نوع النظام System type	ذاكرة الوصول العشوائي RAM
Windows ١٠ pro	Intel(R)Core(TM)i5-2410M CPU @2.30GHz	64-bit	4GB

قيمت السلاسل الثنائية من خلال اختبار NIST لاختبار العشوائية [23]، ومن خلال مسافة هامينغ لاختبار التميز والتفرد[11].

المخطط المقترح :

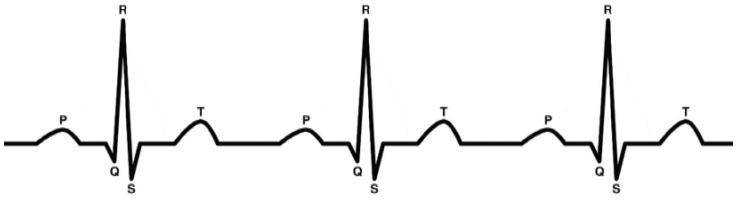
سنورد فيما يأتي خطوات المخطط المقترح لتوليد مفاتيح تشفير بطول ١٠٢٤ بت:

٤-١. استخلاص مميزات إشارة ECG:

نبين فيما يأتي الخطوات التي اتُّبعت لتوليد سلسلة بتات عشوائية من مميزات إشارة ECG بالاعتماد على قاعدة البيانات MIT_BIH Arrhythmia :

١- من أجل تسجيل معين، حُصلِّت إشارة ECG لمدة زمنية بحيث تتضمن ٣ نبضات قلب كاملة .

٢- استخلاص ثلاث نبضات قلب (PQRST) متتالية من التسجيل السابق كما هو موضح .



الشكل(١): تتابع ثلاث نبضات من إشارة ECG

٣- تطبيق خوارزمية XQRS لتحديد مواقع القمم R في النبضات المحصلة.

تعد خوارزمية XQRS أحد الأصناف المضمنة في الحزمة البرمجية WFDB، إذ تكتشف وتحدد موقع القمة R في التعقيد QRS ضمن إشارة ECG . تمتلك هذه الخوارزمية ميزة إضافية وهي تطبيق مرشح تمرير حزمة للإشارة بين Hz (20-5) [20]. ومنه سنحصل على مواقع القمم (R1 , R2 , R3).

٤- تطبيق تابع diff للحصول على RR-interval . ومنه سينتج لدينا (R1R2 , R2R3).

٥- من أجل كل نبضة قلب كاملة PQRST استُخلصت مواقع القمم P,Q,R,S,T وحُسبَ الوسيط mean . ومن ثم حساب الفروقات بين القمم : PQ, QR, RS, ST, RT, PR .

٦- تحويل جميع القيم التي حُصلَ عليها من أجل نبضات PQRST الثلاثة إلى الصيغة الثنائية.

ترتيبها وفق آلية معينة للحصول على سلسلة ثنائية بطول 381 بت .

٧- من أجل هذه السلسلة الثنائية حُشرت بتات إضافية ضمنها وفق آلية معينة تتضمن عملية XOR للحصول على سلسلة ثنائية بطول 508 بت، ومن ثم إضافة الترميز الثنائي للعدد 3 ممثلاً بأربع خانات، ومنه سنحصل على سلسلة ثنائية مكونة من 512 بت كما هو موضح في الشكل (٢).

B1	B2	B3	C1	B4	B5	B6	C2	.....	C508	0011

$C_1 = B_1 \text{ xor } B_2 \text{ xor } B_3$ $C_2 = B_4 \text{ xor } B_5 \text{ xor } B_6$

الشكل(٢): السلسلة الثنائية بطول 512 بت المشكلة من مميزات ECG

٤-٢. استخلاص مميزات إشارة EEG:

اعتمدنا في دراستنا على قاعدة البيانات EEG Motor Movement/Imagery Dataset V1.0.0، والتي تضم تسجيلات EEG لـ ١٠٩ أشخاص مشاركين ، حيث تتضمن ٤ مهام و ١٤ جولة تجريبية. سُجلت إشارات تخطيط الدماغ للمشاركين باستخدام ٦٤ قناة وهم يقومون بمهام تخيل الحركة (MI) وذلك بالاعتماد على المعيار BCI2000 باستخدام نظام ١٠-١٠ الدولي بمعدل أخذ عينات ١٦٠ هرتز.

أولاً: المعالجة الأولية (preprocessing):

تتضمن الخطوات الآتية:

١- **اختيار القناة** : تُختار قنوات EEG الأكثر ملاءمة لمهام تخيل الحركة (MI)، حيث يفضل استخدام عدد أقل من قنوات EEG من أجل تقليل التكلفة الحسابية والذاكرة المطلوبة وتخفيض تعقيد النظام وتكلفة المعدات اللازمة عند وضع الأقطاب الكهربائية. ولكن يجب الأخذ بالحسبان وضع هذه الأقطاب

في المكان المناسب تجنباً لفقدان معلومات مفيدة، لذلك يجب اختيار العدد الأمثل للأقطاب الكهربائية والمواضع المناسبة لها. اخترنا في بحثنا هذا ٦ قنوات فقط وهي موجودة في منطقة القشرة الحسية الحركية (FC1 , FC2 , FC3 , FC4 , FC5 , FC6) وهي المسؤولة عن إشارات تخيل الحركة.

٢- **ترشيح الإشارة:** اختير النطاق الترددي الأكثر ملاءمة لمهام MI، حيث بينت الدراسات بالنسبة لإشارات تخيل الحركة تحدث التغيرات في الطاقة للإيقاعات الحسية الحركية بشكل رئيسي في نطاقي الترددات (α وβ) لذلك استخدمنا في دراستنا مرشح تمرير حزمة Hz(40-0) . تتضمن هذه المرحلة أيضاً ترشيح وإزالة الإشارات غير المرغوب فيها وإشارات الضجيج الناجمة عن الحركات الإرادية وضجيج مخطط كهربائية العضلات، وضجيج إشارات العين من خلال المكتبة البرمجية mne والتي تتيح توابع خاصة بإزالة هذه الإشارات.

٣- **إزالة الشوائب:** بالرغم من استخدام مرشح تمرير حزمة إلا أنه يبقى من الصعب استبعاد جميع الشوائب، لذلك طبقنا التابع البرمجي del- annotation لحذف الإشارات غير المرغوبة وغير المفيدة.

ثانياً: استخراج المميزات :

تحوي إشارات تخطيط الدماغ ضمن مميزاتها الزمنية والترددية معلومات مفيدة تعبر عن هذه الإشارات، لذا اعتمدنا في دراستنا على استخراج بعض هذه المميزات، والتي تَعدّ من أهم المميزات المعتمدة في الأبحاث والدراسات عند دراسة النشاط الكهربائي للدماغ وهي [13]:

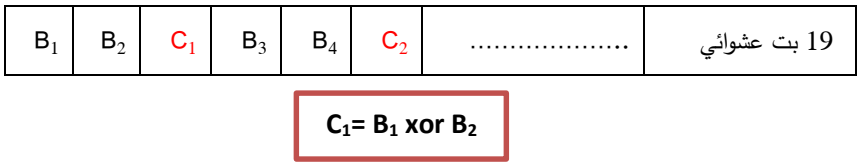
المميزات الزمنية : المتوسط الحسابي (Mean) ، الانحراف المعياري(Standard Deviation)، معامل اللاتماثل أو التجانف(Skewness) ، معامل التسطح أو درجة التقوس(Kurtosis).

المميزات الترددية : درسنا الكثافة الطيفية للطاقة PSD (power spectral density) والتي تمثل كيفية توزيع طاقة الإشارة أو السلسلة الزمنية مع التردد، وتُستخدم هذه المميزة في عمليات التصنيف والترميز.

ثالثاً: تشكيل سلاسل الأرقام الثنائية:

بعد أن أجرينا المعالجة الأولية لإشارات تخطيط الدماغ، حصلنا على ملفات تتضمن إشارات تخطيط الدماغ الخاصة بتخيل الحركة MI-EEG. ومن ثم استخرجنا **المميزات الزمنية** التي عرفناها سابقاً، وجمعنا هذه المميزات الأربعة للقنوات الستة، ومن أجل **المميزات الترددية** ، قسمنا النطاق الترددي إلى ٥ مجالات ترددية، واستخرجنا الطاقة العظمى لكل نطاق ترددي على حدا من خلال خوارزمية التقدير welch والتي تستخدم لتقدير معاملات النماذج الإحصائية عندما تكون بعض البيانات مفقودة أو غير مرئية. ومن ثم جمعنا المميزات الزمنية مع المميزات الترددية لـ ١٠٠٠٠ عينة مدروسة وحولناها إلى الصيغة الثنائية، فحصلنا على سلاسل ثنائية طول كل منها ٣٢٩ بت.

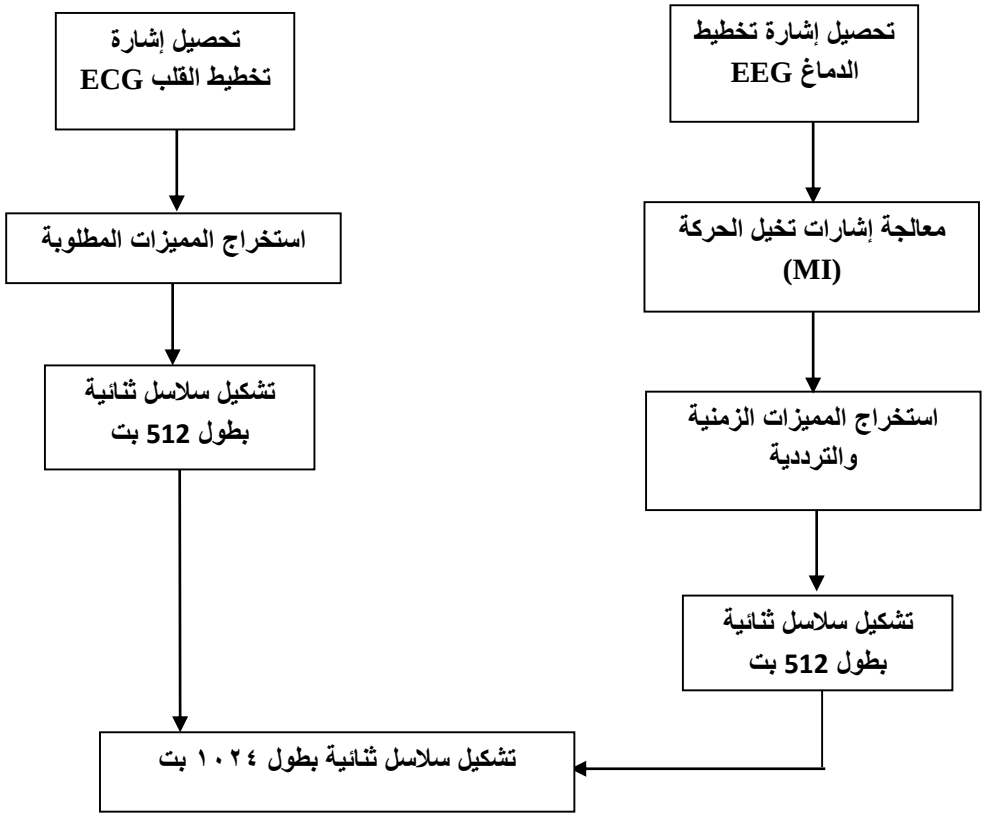
بعد ذلك أجرينا عملية حشر لبتات ضمن كل سلسلة، من خلال إجراء عملية xor لكل خانتين متتاليين وحشر النتيجة في الخانة الثالثة، وهكذا تتكرر العملية للحصول على سلسلة ثنائية بطول ٤٩٣ بت، ومن ثم إضافة 19 بت مختارة بشكل عشوائي فيصبح الناتج ٥١٢ بت لكل سلسلة، لنحصل بالنتيجة على ١٠٠٠٠سلسلة ثنائية طول كل منها ٥١٢ بت، كما هو موضح في الشكل (3):



الشكل(3): السلسلة الثنائية بطول 512 بت المشكلة من مميزات EEG

٤-٣. تشكيل السلاسل الثنائية من العلامات الحيوية الهجينة:

تمكنا مما سبق من تشكيل سلاسل ثنائية كل منها بطول ٥١٢ بت، وذلك من خلال استخلاص مميزات كل من إشارتي ECG و EEG ومعالجتها وتحويلها إلى الصيغة الثنائية وفق ترتيب معين، بعد ذلك سنقوم بدمج ناتج مميزات هاتين العلامتين الحيويتين بالتناوب للحصول على سلاسل ثنائية كل منها بطول ١٠٢٤ بت. ويبين الشكل (4) خطوات المخطط المقترح:



الشكل(٤):مخطط توليد مفاتيح التشفير المقترح

النتائج والمناقشة:

تمكنا من خلال المخطط المقترح سابقاً من الحصول على سلاسل ثنائية كل منها بطول ١٠٢٤ بت، وفيما يأتي سنقيم هذه السلاسل من خلال عدة إحصائيات معتمدة عالمياً لمعرفة إمكانية استخدامها كسلاسل عشوائية في التطبيقات الأمنية وغيرها.

٥-١. اختبار العشوائية:

يوجد العديد من الاختبارت التي تدرس عشوائية السلاسل الثنائية، اعتمدنا في بحثنا على هذا الاختبار NIST الذي يُعدّ من أهمها، لأنه مخصص لدراسة عشوائية السلاسل المستخدمة لأغراض التشفير وحماية البيانات.

يتضمن اختبار NIST اختبارات طورت لدراسة عشوائية السلاسل الثنائية المولدة من عتاد صلب أو برمجي بالاعتماد على مولدات الأرقام العشوائية أو شبه العشوائية [23].

طبقنا اختبارات NIST على ١٠٠ سلسلة ثنائية مولدة وفق المخطط الذي اقترحناه سابقاً.

يُحدد الحد الأدنى لعدد الاختبارات الواجب اجتيازها لكل من اختبارات NIST وفق المعادلة الآتية [28]:

$$mpr = (1-\alpha) - 3\sqrt{\frac{\alpha(1-\alpha)}{k}} \qquad (١)$$

حيث، α تمثل مستوى الأهمية وهنا تأخذ القيمة 0.01 ، أما k فيمثل عدد السلاسل المختبرة وهنا $k = 100$.

ومنه يكون الحد الأدنى للنجاح هو % 96 . أي من أجل كل اختبار يجب أن يكون عدد السلاسل الناجحة (العشوائية) هو ٩٦ سلسلة أو أكثر من أصل ١٠٠ سلسلة مختبرة.

ينتج عن كل اختبار قيمة لـ P والتي من خلالها يُحدد فيما إذا كانت السلسة عشوائية أم لا. فإذا كانت قيمة P الناتجة أكبر من قيمة α تكون السلسلة عشوائية وعدا ذلك تكون غير عشوائية. يبين الجدول (٢) نتائج الاختبارات التي نفذناها باستخدام اختبار NISTSP800-22 [24]:

الجدول (٢): يمثل نتائج اختبارات NIST

الاختبار	P	نسبة النجاح	النتيجة
The frequency(monobit)test	0.472	99%	pass
Frequency test within a block	0.698	100%	Pass
The Runs test	0.416	98%	Pass
The longest Run of ones in a block	0.501	96%	Pass
The discrete Fourier Transform test	0.662	99%	Pass
The Approximate Entropy test	0.439	96%	Pass
The cumulative sum test(Forward)	0.604	97%	Pass
The cumulative sum test(backward)	0.335	97%	Pass
The serial test	0.٢٩١	96%	Pass

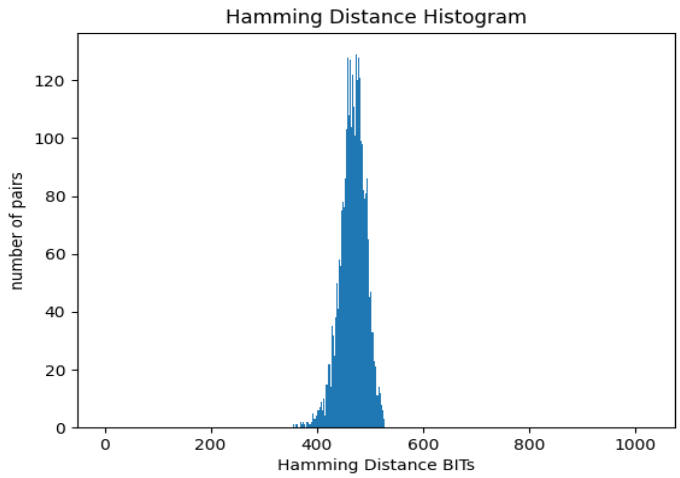
نلاحظ من الجدول السابق أن السلاسل الثنائية المولدة وفق المخطط المقترح قد اجتازت جميع الاختبارات ويمكن أن نحكم عليها بأنها سلاسل عشوائية.

٥-٢. اختبار التميز (التفرد):

نعتمد على هذه الإحصائية لتحديد مدى التميز (الاختلاف) بين السلاسل العشوائية المولدة من أجسام مختلفة، وتقاس هذه الإحصائية من خلال مسافة هامينغ (HD(Hamming Distance والتي تحسب عدد المواضع المختلفة بين كل سلسلتين. بالنسبة للسلاسل الثنائية يجب أن تكون مسافة هامينغ تابعة للتوزع الطبيعي ومنه يجب أن يكون متوسط مسافة هامينغ مساوياً تقريباً لـ 50% من طول السلسلة العشوائية[11].

من أجل تطبيق مسافة هامينغ ولدنا ملف يحوي ١٢٠ سلسلة عشوائية، وحسبنا مسافة هامينغ بين هذه السلاسل فحصلنا على النتيجة الموضحة في الشكل (٥)، حيث يمثل المحور الأفقي مسافة هامينغ مقدرة بالبت، والمحور الشاقولي يمثل عدد الأزواج التي تمتلك نفس مسافة هامينغ.

نلاحظ من الشكل السابق التوزع الطبيعي لمسافة هامينغ، إذ أن متوسط HD يساوي ٤٥,٩ % وهو قريب جداً من ٥٠% من طول السلسلة العشوائية، ومنه نستنتج أن السلاسل المولدة وفق المخطط المقترح في بحثنا هذا فريدة ومتمايزة .



الشكل(٥): مسافة هامينغ للسلاسل الثنائية المولدة

٥-٣. تطبيق المفاتيح الناتجة مع خوارزمية التشفير AES :

تمكنا من خلال المخطط الذي اقترحناه من تشكيل سلاسل بتات عشوائية بطول ١٠٢٤ بت، ومن خلال الاختبارات التي أجريناها تبين معنا عشوائية هذه السلاسل وتمايزها ، سنجري في هذه الفقرة تطبيقاً عملياً لهذه السلاسل، حيث سنستخدمها كمفاتيح لتشفير وفك تشفير بيانات وفق خوارزمية التشفير المتناظر AES-GCM(Advanced Encryption Standard – Galois Counter Mode) [25] .

النص الصريح المراد تشفيره: هذه رسالة سرية جداً سيتم تشفيرها باستخدام سلسلة بتات ١٠٢٤

مفتاح التشفير:

ويبين الشكل الآتي نتيجة عملية التشفير وفك التشفير وفق خوارزمية AES من أجل إحدى السلاسل العشوائية:

الشكل(٦) : مثال عن عمليتي التشفير وفك التشفير

```
--- بدء عملية التشفير ---
[تشفير] تحويل سلسلة البتات (1024 بت) إلى بايتات...
[تشفير] تم تحويل المفتاح إلى 128 بايت.
[تشفير] تم توليد Salt: ebb18549652182404c536fe3b073e293
[KDF] جاري اشتقاق مفتاح AES-256...
[KDF]   Salt المستخدم (hex): ebb18549652182404c536fe3b073e293
[KDF]   Info المستخدم: bio_key_aes_gcm_encryption_v2
[KDF]   تم اشتقاق مفتاح AES (hex): 74aabe4a2913534eb23e5c2ffe276b45a508129a2b497b08cba3b2c4aaa873e8
[تشفير] تم توليد Nonce: a83e95b49e072e74736fc729
[تشفير] جاري تشفير النص: 'هذه رسالة سرية جداً سيتم تشفيرها باستخدام سلسلة بتات 1024'.
[تشفير] تم التشفير بنجاح.
[تشفير] النص المشفر (مع التاغ) (hex): 386f1eed3088ba332549eb6f5413de2602534277d869ef615ab96d42b45e205da2a6a9ce121dc1bb0f907568627bae5eaf9a386a82ec07348cd163caa
20a2213218f488b4b2c59658e413ec3491e6dbff1e92991306d8939f9394bac86f9013bf761520cd594ade5956203722c63b9eeb826476e19c0

--- بدء عملية فك التشفير ---
[فك التشفير] تحويل سلسلة البتات (1024 بت) إلى بايتات...
[فك التشفير] تم تحويل المفتاح إلى 128 بايت.
[KDF] جاري اشتقاق مفتاح AES-256...
[KDF]   Salt المستخدم (hex): ebb18549652182404c536fe3b073e293
[KDF]   Info المستخدم: bio_key_aes_gcm_encryption_v2
[KDF]   تم اشتقاق مفتاح AES (hex): 74aabe4a2913534eb23e5c2ffe276b45a508129a2b497b08cba3b2c4aaa873e8
[فك التشفير] جاري فك التشفير والتحقق من التاغ...
[فك التشفير]   باستخدام Nonce: a83e95b49e072e74736fc729
[فك التشفير] تم فك التشفير والتحقق بنجاح

--- نتيجة فك التشفير ---
الرسالة الأصلية المفكوكة: هذه رسالة سرية جداً سيتم تشفيرها باستخدام سلسلة بتات 1024.
```

الاستنتاجات و التوصيات :

تمكنا في بحثنا هذا من توليد سلاسل بتات اعتماداً على الدمج ما بين مميزات إشارة تخطيط القلب ECG و إشارة تخطيط الدماغ الخاصة بتخيل الحركة EEG-MI، حيث أجرينا المعالجة الأولية لهذه الإشارات، ومن ثم وضعنا آلية معينة لاستخلاص المميزات المفيدة من هذه الإشارات وترتيبها وفق نمط معين لتشكيل سلاسل ثنائية بطول ١٠٢٤ بت. يتمتع المخطط المقترح في بحثنا بما يأتي:

١- أكثر فعالية من الدراسات السابقة من ناحية الإنتاجية، فمن أجل إشارة تخطيط القلب تمكنا من تشكيل سلاسل ثنائية بطول ٥١٢ بت انطلاقا من ثلاث نبضات قلب أي وسطيا (٣ – ٥) ثانية من تسجيل ECG بينما احتاجت الأبحاث السابقة لـ ٣٣ ضربة قلب أي ما يعادل ٢٠ إلى ٣٠ ثانية لتشكيل سلسلة بطول ١٢٨ بت، وبعض الدراسات استخدمت نبضة قلب وحيدة ولكن أنتجت فقط ١٦ بت.

ومن أجل إشارة تخطيط الدماغ اعتمدنا في بحثنا على ٦ الكترودات فقط موجودة ضمن منطقة القشرة الحسية الحركية، والتي كانت كافية لتزويدنا بالمعلومات المفيدة المطلوبة. إذ استغرقت التجربة المستخدمة فقط ٤ ثواني، وتمكنا من خلالها توليد سلاسل بطول ٥١٢ بت. لذا نجد أن هذا المخطط حقق إنتاجية أعلى خلال زمن أقل.

٢- أخضعت السلاسل الناتجة عن هذا المخطط لاختبار العشوائية NIST وقد تبين معنا أن هذه السلاسل قد اجتازت الاختبارات القابلة للتطبيق من أجل سلاسل بطول ١٠٢٤ بت.

٣- درسنا مسافة هامينغ للسلاسل الثنائية لمعرفة مدى التميز، وقد تبين أن هذه السلاسل متمايزة وفريدة ، وهذا يضمن عدم القدرة على التنبؤ بمميزات إشارات ECG و EEG لشخص ما من معرفة مميزات هذه الإشارات لشخص آخر.

٤- فعالية عالية من ناحية تعقيد النظام والتكلفة، إذ يتمتع المخطط المقترح ببساطة العمليات المستخدمة حيث لم يتم استخدام توابع رياضية معقدة أو تخضع السلسلة لأي نوع من الترامیز التي قد تستهلك موارد الشبكة المحدودة إذ أنه بعد استخلاص المميزات استخدمنا فقط عملية XOR والتي تعد من أبسط العمليات المنطقية.

مما سبق نستنتج فعالية استخدام إشارات تخطيط القلب والدماغ معاً كعلامات حيوية في توليد أرقام عشوائية، إذ يمكن اعتبار هذه الإشارات مصدراً للأرقام العشوائية الصحيحة ، أو يمكن استخدامها كدخل لمولدات الأرقام شبه العشوائية . ونستنتج أيضاً أن السلاسل الثنائية المولدة وفق المخطط المقترح في هذا البحث يمكن استخدامها كمفاتيح تعمية في شبكات WBSNs وغيرها من التطبيقات الأمنية، إذ أن هذه السلاسل تتميز بالعشوائية والخصوصية التامة، وتمتلك الطول المناسب لتطبيقها مع خوارزميات التشفير الشهيرة. إضافة إلى أنها لا تستهلك موارد الشبكة المحدودة.

نقترح في نهاية بحثنا دراسة إمكانية تطوير المخطط المقترح هنا لتوليد سلاسل بتات عشوائية من خلال إشارات تخطيط الدماغ والقلب بفعالية أكبر مستفيدين من تقنيات الذكاء الصنعي. ووضع آليات معينة للاستفادة من السلاسل الثنائية الناتجة عن هذه العلامات الحيوية لاستخدامها كمفاتيح تعمية في شبكات WBSNs .

المراجع:

[1] YAGHOUBI, M.; AHMED, K. and MIAO, Y., *Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges*. Intelligent Technology Innovation Lab (ITIL), Victoria University, Ballarat Road, Footscray, Melbourne, VIC 3011, Australia, Vol.11, Issue 4, 2022.

[2] KAUR, P.; KUMAR, N. and SINGH, M., *Biometric cryptosystem: a comprehensive survey*. Multimed Tools Appl, Vol.82, PP.16635-16690, 2023.

[3] RAKHMATULIN, I.; DAO, M.; MANDIC, D. and NASSIBI, A., *Exploring Convolutional Neural Network Architectures for EEG Feature Extraction*, sensors, 2024.

[4] SAIFUL ISLAM, M. *Using ECG signal as an entropy source for efficient generation of long random bit sequences.* Journal of King Saud University – Computer and Information Sciences, 2022.

[5] SINHA, A.; MAHAPATRO, J. and BHABANI, B., *Random binary sequences generation using heartbeats for cryptographic keys in WBSNs*. International Journal of Sensor Networks, Vol.38, No.3, PP.191-203, 2022.

[6] PREMKUMAR, S. and MOHANA, J., *An efficient method for Secure ECG Feature Based Cryptographic Key Generation*. IJITEE, Vol.8, 8 Issue-12, PP.159-164, 2019.

[7] XU, F.; Qin, Z.; Tan, C.; Wang, B. and Li, Q., *IMDGuard: Securing implantable medical devices with the external wearable guardian*. IEEE INFOCOM, pp. 1862–1870, 2011.

[8] ZHENG, G.; FANG, G.; SHANKARAN, R.; ORGUN, M.; SALEEM, K.; and QIAO, L., *Multiple ECG Fiducial Points based Random Binary Sequence Generation for Securing Wireless Body Area Networks.* IEEE Journal of Biomedical and Health Informatics, Vol. 21, No. 3, PP.655–663.2017.

[9] CHEN, G., *Are electroencephalogram (EEG) signals pseudo-random number generators?*, J. Comput. Appl. Math. 268, PP.1– 4 , 2014.

[10] NGUYEN, D.; TRAN, D.; MA, W. and NGUYEN, Kh., *EEG-Based Random Number Generators.* Springer International Publishing AG, PP. 248-256, 2017.

[11] BAJWA, G. and DANTU, R., *Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms,* ScienceDirect, No. 62, PP.95 – 113, 2016.

[12] KUMAR, P.; SAINI , R.; KAUR , B.; ROY, P. and SCHEME, E., *Fusion of Neuro-Signals and Dynamic Signatures for Person Authentication,* sensors, Vol. 19, No. 4641, 2019.

[13] RAHMAN, A.; CHOWDHURY, M.; KHANDAKAR, A.; KIRANYAZ,S. and et al, *Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms*, IEEE, Vol. 2017, 2021.

[14] ZEYNALI, M.; SEYEDARABI, H. and TAZEHKAND, M., *Development of a Unique Biometric-based Cryptographic Key Generation with Repeatability using Brain Signals*, Journal of AI and Data Mining, Vol. 8, No. 3, PP.343-

356, 2020.

[15] DAS, R.; MAIORANA, E. and P. CAMPISI, P., *Motor imagery for EEG biometrics using convolutional neural network*, in Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2062–2066, IEEE, Calgary, Canada, April 2018.

[16] BAK, S. and JEONG, J., *User Biometric Identification Methodology via EEG-Based Motor Imagery Signals*, IEEE, Vol. 2017-0-00451, 2023.

[17] Nguyen, D.; Tran, D.; Sharma, D. and Ma, W., On *the study of EEG-based cryptographic key generation*, Procedia Computer Science, vol. 112, PP. 936–945, 2017.

[18] DAMAŠEVIIIUS, R.; MASKELINAS, R.; KAZANAVIIIUS, E. and WOFNIAK, M., *Combining Cryptography with EEG Biometrics***,** Computational Intelligence and Neuroscience, 2018.

[19] MIT-BIH Arrhythmia Database. https://physionet.org/content/mitdb/1.0.0/ Last visit at April 2025.

[20] https://wfdb.readthedocs.io/en/latest/index.html . Last visit at April 2025

[21] EEG Motor Movement/Imagery Dataset. https://physionet.org/content/eegmmidb/1.0.0/. Last visit at April 2025.

[22] https://www.python.org/downloads/release/python-31011/. Last visit at April 2025.

[23] RUKHIN, A.; SOTO, J.; NECHVATAL, J.; SMID, M. and BARKER, E., *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Natl. Inst. Standards Technol., Gaithersburg, USA, Tech. Rep. 800-22rev1a, 2010.

[24] https://github.com/stevenang/randomness_testsuite . Last visit at April 2025.

[25] SUNG, B.; KIM, K. and SHIN, K., *An AES-GCM authenticated encryption crypto-core for IOT security*, 2018 international conference on Electronics, information, and communication (ICEIC), Honolulu, HI, USA, pp.1-3, 2018.