الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

المعايير الوطنية للتشفير

National Cryptographic Standards

(NCS – 1: 2020)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

التحديثات على الوثيقة

الإصدار	التاريخ	التغييرات
١,٠	يوليو ٢٠٢٠	النسخة الأولى

قائمة المحتويات

	التحديثات على الوثيقة	٥
	الملخص التنفيذي	٨
١	**المقدمة**	**٩**
١,١	النطاق	٩
١,٢	مستويات معايير التشفير	٩
١,٣	هيكلية الوثيقة	١٠
٢	**أساسيات التشفير CRYPTOGRAPHIC PRIMITIVES**	**١١**
٢,١	الخوارزميات المتماثلة SYMMETRIC ALGORITHMS	١١
٢,١,١	خوارزميات التشفير الانسيابية Stream Cipher Algorithms	١١
٢,١,٢	خوارزميات التشفير الكتلية Block Ciphers Algorithms	١١
٢,٢	الخوارزميات غير المتماثلة ASYMMETRIC ALGORITHMS	١٢
٢,٣	دوال الاختزال HASH FUNCTIONS	١٢
٢,٤	خوارزميات التشفير الخفيفة LIGHTWEIGHT CRYPTO ALGORITHMS	١٢
٣	**تصاميم التشفير CRYPTOGRAPHIC SCHEMES**	**١٤**
٣,١	طرق عمليات التشفير الكتلية BLOCK CIPHER MODES OF OPERATION	١٤
٣,٢	رموز توثيق الرسائل MESSAGE AUTHENTICATION CODES (MAC)	١٤
٣,٣	التشفير والتوثيق باستخدام البيانات المرتبطة AUTHENTICATED ENCRYPTION WITH ASSOCIATED DATA (AEAD)	١٤
٣,٤	دوال حماية المفاتيح KEY WRAP FUNCTIONS	١٥
٣,٥	دوال اشتقاق المفاتيح KEY DERIVATION FUNCTIONS (KDF)	١٥
٣,٦	الاتفاق على المفاتيح ونقلها KEY AGREEMENT AND KEY TRANSPORT	١٥
٣,٦,١	التصاميم المتماثلة Symmetric Schemes	١٥
٣,٦,٢	التصاميم غير المتماثلة Asymmetric Schemes	١٥
٣,٧	تصاميم التشفير الهجينة HYBRID ENCRYPTION SCHEMES	١٦
٣,٨	تواقيع المفاتيح العامة PUBLIC KEY SIGNATURES	١٦

٤ بروتوكولات التشفير الشائعة
COMMONLY USED CRYPTOGRAPHIC PROTOCOLS ١٨
٤,١ بروتوكول الإنترنت الآمن IP SECURITY (IPSEC) ١٨
٤,٢ بروتوكول طبقة النقل الآمنة TRANSPORT LAYER SECURITY (TLS) ١٨
٤,٣ بروتوكول نظام اسم النطاق الآمن DOMAIN NAME SYSTEM SECURITY (DNSSEC) ١٩
٤,٤ بروتوكول الاتصال الآمن عن بعد SECURE SHELL (SSH) ١٩
٤,٥ بلوتوث BLUETOOTH ١٩
٤,٦ نظام الاتصالات المتنقلة العالمية (UMTS) / الجيل الرابع (LTE) / الجيل الخامس (5G) ٢٠
٤,٧ الوصول الآمن للشبكة اللاسلكية WPA (WI-FI PROTECTED ACCESS) ٢٠
٤,٨ بروتوكول كيربيروس KERBEROS PROTOCOL ٢٠
٥ البنية التحتية للمفاتيح العامة PUBLIC KEY INFRASTRUCTURE (PKI) ٢١
٥,١ خوارزميات الشهادات ALGORITHMS FOR CERTIFICATES ٢١
٥,٢ صلاحية الشهادات VALIDITY OF THE CERTIFICATES ٢١
٦ إدارة دورة المفاتيح KEY LIFECYCLE MANAGEMENT (KLM) ٢٢
٦,١ حماية المفاتيح وصلاحيتها KEY PROTECTION AND LIFETIME ٢٢
٦,٢ عمليات إدارة دورة المفاتيح KLM PROCESSES ٢٢
٧ الملحقات ٢٥
٧,١ توليد الأعداد شبه العشوائية PSEUDO RANDOM NUMBER GENERATION (PRNG) ٢٥
٧,٢ التشفير ما بعد الحوسبة الكمية POST-QUANTUM CRYPTOGRAPHY ٢٥
٧,٣ هجمات القنوات الجانبية SIDE-CHANNEL ATTACKS ٢٦
٧,٤ تعريفات ٢٧
٧,٥ قائمة الاختصارات ٣٢

الملخص التنفيذي

تهدف الهيئة الوطنية للأمن السيبراني إلى تعزيز الأمن السيبراني حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، كما ورد في تنظيم الهيئة الصادربالأمر الملكي الكريم رقم ٦٨٠١، وتاريخ ١٤٣٩/٢/١١هـ والذي تضمن مهام واختصاصات الهيئة وأنها الجهة المختصة في المملكة العربية السعودية بالأمن السيبراني والمرجع الوطني في شؤونه.

وقد اشتمل تنظيم الهيئة على اختصاصها بوضع السياسات والمعايير الوطنية للتشفير، ومتابعة الالتزام بها، وتحديثها. و من هذا المنطلق، أعدت الهيئة الوطنية للأمن السيبراني المعايير الوطنية للتشفير (NCS - 1: 2020) لتحديد الحد الأدنى من متطلبات التشفير للأغراض المدنية والتجارية وذلك لحماية البيانات والأنظمة والشبكات الوطنية. تسلط هذه الوثيقة الضوء على تفاصيل معايير التشفير الوطنية والتي تتكون من مستويين من القوة: أساسي ومتقدم.

تحدد هذه الوثيقة أساسيات التشفير التماثلية وغير التماثلية المقبولة Accepted Symmetric and Asymmetric Primitives ، وتصاميم التشفير التماثلية وغير التماثلية المقبولة Accepted Symmetric and Asymmetric Schemes ، وبعض بروتوكولات التطبيقات الشائعة المقبولة ذات العلاقة بالتشفير Accepted Common Application Protocols related to Cryptography ، والبنية التحتية للمفاتيح العامة Public Key Infrastructure (PKI) ، وإدارة دورة المفاتيح Key Lifecycle Management (KLM)، بالإضافة إلى ملحقات تتناول توليد الأعداد شبه العشوائية Pseudo Random Number Generation (PRNG) ، والتشفير ما بعد الحوسبة الكمية Post-Quantum Cryptography وهجمات القنوات الجانبية Side-channel Attacks.

١ المقدمة

١,١ النطاق

إن الهيئة الوطنية للأمن السيبراني تحدد في هذه الوثيقة الحد الأدنى لمتطلبات التشفير للأغراض المدنية أو التجارية لكي يتم الالتزام بها من قبل الجهات الوطنية بما يضمن استخدام أنظمة التشفير المناسبة. ومن المهم جدا أن يضمن الملتزمون بهذه المعايير التطبيق الصحيح والآمن لها وذلك لتفادي الثغرات الناتجة عن أخطاء التطبيق.

تم الأخذ بالاعتبار عند إعداد وثيقة المعايير الوطنية للتشفير الوضع الراهن والتقدم المتوقع في القدرات الحوسبية مع افتراض عدم وجود قدرات الحوسبة الكمية. تشمل هذه الوثيقة أساسيات التشفير Cryptographic Primitives، وتصاميم التشفير Cryptographic Schemes، وبروتوكولات التشفير الشائعة Commonly used Cryptographic Protocols، والبنية التحتية للمفاتيح العامة Public Key Infrastructure (PKI)، وإدارة دورة المفاتيح Key Lifecycle Management (KLM).

هذه الوثيقة التي نطلق عليها المعايير الوطنية للتشفير (NCS - 1: 2020) تحدد الحد الأدنى من متطلبات التشفير للأغراض المدنية والتجارية وذلك لحماية البيانات (عند تخزينها أو معالجتها أو نقلها) والأنظمة والشبكات الوطنية. وسيتم تحديث هذه الوثيقة عند الحاجة بحسب المستجدات في مجال التشفير. ويلغي كل إصدار جديد من هذه الوثيقة كافة الإصدارات السابقة.

١,٢ مستويات معايير التشفير

تحدد المعايير الوطنية للتشفير مستويين اثنين من مستويات القوة لمعايير التشفير، وهي المستوى الأساسي MODERATE والمستوى المتقدم ADVANCED ، وذلك لضمان مرونة التنفيذ وكفاءته. وقد تم تصميم مستويات القوة لتستهدف مستوى أمن 128 -بت بالنسبة للمستوى الأساسي ومستوى أمن 256 -بت بالنسبة للمستوى المتقدم. وعلى كل جهة اختيار وتطبيق مستوى التشفير المناسب حسب طبيعة ومستوى حساسية البيانات والأنظمة والشبكات المراد حمايتها. وبالإضافة لذلك، تحدد وثائق أخرى تصدر من الهيئة الوطنية للأمن السيبراني تتعلق بضوابط وسياسات الأمن السيبراني التخصيص المناسب لمستوى القوة الذي يجب الالتزام به من قبل الجهات الوطنية لحماية البيانات والأنظمة والشبكات. وقد تم تحديد متطلبات محددة لكل مستوى من المستويين أعلاه في هذه الوثيقة، وفي حال الإشارة إلى متطلب غير مرتبط بمستوى قوة محدد فسينطبق هذا المتطلب على كلا المستويين معا.

١,٣ هيكلية الوثيقة

تـم تنظيـم بقيـة هـذه الوثيقـة عـلى النحـو التـالي: يعـرض القسـم ٢ مـن هـذه الوثيقـة أساسـيات التشـفير المقبولـة Accepted Cryptographic Primitives شـاملة أطـوال المفاتيـح Keys والكتـل Blocks ومتجهـات التهيئـة Initialization Vectors. ويقـدم القسـم ٣ تصاميـم التشـفير المقبولـة Accepted Cryptographic Schemes وتشـمل طـرق عمليـات التشـفير Modes of Operations، ورمـوز توثيـق الرسـائل Message Authentication Code (MAC)، والتشـفير والتوثيـق باسـتخدام البيانـات المرتبطـة Authenticated Encryption with Associated Data (AEAD)، ودوال حمايـة المفاتيـح Key Wrap Functions (KWF)، ودوال اشـتقاق المفاتيـح Key Derivation Functions (KDF)، والاتفـاق عـلى المفاتيـح ونقلهـا Key Agreement and Key Transport، وتصاميـم التشـفير الهجينـة Hybrid Encryption Schemes، وتواقيـع المفاتيـح العامـة Public Key Signatures. كـما يحتـوي القسـم ٤ عـلى متطلبـات التشـفير لبروتوكـولات التطبيقـات الأكـثر شـيوعًا وهـي: بروتوكـول الإنترنـت الآمـن (IPsec)، وبروتوكـول طبقـة النقـل الآمنـة (TLS)، وبروتوكـول نظـام اسـم النطـاق الآمـن (DNSSEC)، وبروتوكـول الاتصـال الآمـن عـن بعـد (SSH)، وبلوتـوث Bluetooth، ونظـام الاتصـالات المتنقلـة العالميـة (UMTS)، والجيـل الرابـع (LTE)، والجيـل الخامـس (5G)، والوصـول الآمـن للشـبكة اللاسـلكية (WPA)، وبروتوكـول كيربـيروس Kerberos Protocol. يعـرض القسـم ٥ قائمـة الخوارزميـات والمتطلبـات للشـهادات وصلاحيتهـا. ويشـمل القسـم ٦ متطلبـات الخطـوات المختلفـة لـدورة المفاتيـح Key Lifecycle لضـمان إدارة المفاتيـح بشـكل آمـن مـن لحظـة إنشـائها حتـى إتلافهـا، ولضـمان الاسـتخدامات المعياريـة لهـا خـلال العمليـات والإجـراءات اللازمـة. وأخـيرًا القسـم ٧ يقـدم ملاحـق تتضمـن توليـد الأعـداد شـبه العشـوائية Pseudo Random Number Generation (PRNG)، والتشـفير مـا بعـد الحوسـبة الكميـة Post-Quantum Cryptography وهجـمات القنـوات الجانبيـة Side-Channel Attacks، والتعريفـات والاختصـارات.

٢ أساسيات التشفير
Cryptographic Primitives

٢,١ الخوارزميات المتماثلة Symmetric Algorithms

٢,١,١ خوارزميات التشفير الانسيابية Stream Cipher Algorithms

الخوارزميات المقبولة:

- SNOW 2.0 (ISO/IEC 18033-4)
  - طول المفتاح 128-بت للمستوى الأساسي.
  - طول المفتاح 256-بت للمستوى المتقدم.
- SOSEMANUK[1] (eSTREAM)
  - طول المفتاح 128-بت و 256-بت للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.

ملاحظات عامة:

- يجب أن يكون طول متجه التهيئة Initialization Vector (IV) على الأقل 128-بت.
- يجب استخدام متجه تهيئة (IV) مختلف لكل مفتاح.
- يجب استخدام المفتاح مرة واحدة فقط.
- فك التشفير بصورة صحيحة لا يعتبر وسيلة للتحقق من الموثوقية Authenticity.

٢,١,٢ خوارزميات التشفير الكتلية Block Ciphers Algorithms

الخوارزميات المقبولة:

- AES (FIPS-197)
  - طول المفتاح 128-بت و 192-بت للمستوى الأساسي.
  - طول المفتاح 256-بت للمستوى المتقدم.
- Camellia (ISO/IEC 18033-3)
  - طول المفتاح 128-بت و 192-بت للمستوى الأساسي.
  - طول المفتاح 256-بت للمستوى المتقدم.
- Serpent [2]
  - طول المفتاح 128-بت و 192-بت للمستوى الأساسي.
  - طول المفتاح 256-بت للمستوى المتقدم.

[1] C. Berbain *et al.* "Sosemanuk, a Fast Software-Oriented Stream Cipher." In: Robshaw M., Billet O. (eds.) New Stream Cipher Designs. LNCS 4986. *Springer*, 2008.

[2] E. Biham, R. Anderson, and L. Knudsen. SERPENT: A new block cipher proposal. In Fast Software Encryption - FSE'98, volume 1372 of Lecture Notes in Computer Science, pages 222–238. *Springer-Verlag*, 1998.

٢,٢ الخوارزميات غير المتماثلة Asymmetric Algorithms

الخوارزميات المقبولة:

- RSA
  - طول المفتاح 3072 بت على الأقل وتكون قيمة "e" أكبر من 65537 للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.
  - يجب استخدام أعداد أولية قوية Strong Primes.
- Diffie-Hellman
  - طول المفتاح 3072 بت على الأقل وتكون قيمة "q" (مجموعة فرعية) 256 للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.
- ECDLP
  - المنحنيات NIST P-256 و NIST P-384 و BrainpoolP256r1 و BrainpoolP384r1 و Curve25519 للمستوى الأساسي.
  - المنحنيات NIST P-521 و Curve448[3] و BrainpoolP512r1 للمستوى المتقدم.

٢,٣ دوال الاختزال Hash Functions

الخوارزميات المقبولة:

- SHA-2
  - SHA-384 و SHA-512/256 للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.
- SHA-3
  - SHA3-256 و SHA3-384 و SHAKE128 و SHAKE256 للمستوى الأساسي.
  - SHA3-512 للمستوى المتقدم.

ملاحظات عامة:

- دوال الاختزال يجب أن تكون مقاومة للانعكاس Inversion Resistant ومقاومة للتعارض Collision Resistant ومقاومة لإيجاد أصل الصورة Pre-image Resistant.
- بالنسبة للخوارزمية SHAKE128، يجب أن يكون حجم مخرجاتها "d" أكبر من أو يساوي 256 بت.
- بالنسبة للخوارزمية SHAKE256، يجب أن يكون حجم مخرجاتها "d" أكبر من أو يساوي 512 بت.
- SHA2-384 وSHA2-512/256 تكتب أحياناً SHA-384 و SHA-512/256 على التوالي.

[3] المنحنى Curve448 مقبول للمستوى المتقدم مع أنه يعمل بمستوى أمن 224 -بت بسبب جودة أدائه ومقاومته لمجموعة كبيرة من هجمات القنوات الجانبية وسهولة تنفيذه.

٢,٤ خوارزميات التشفير الخفيفة Lightweight Crypto Algorithms

الخوارزميات المقبولة (على الأنظمة المحدودة ذات الموارد المقيدة، حيث يكون استخدام معايير التشفير التقليدية غير فعال):

- خوارزميات التشفير الكتلية Block Ciphers (ISO 29192-2)
  - PRESENT طول المفتاح 80-بت أو 128-بت.
  - CLEFIA طول المفتاح 128-بت أو 192-بت أو 256-بت.
- خوارزميات التشفير الانسيابية Stream Ciphers (ISO 29192-3)
  - Enocoro طول المفتاح 80-بت أو 128-بت.
  - Trivium طول المفتاح 80-بت.
- الخوارزميات غير المتماثلة Asymmetric Algorithms (ISO 29192-4)
  - Unilateral
  - ALIKE
  - Identity-based signature
- دوال الاختزال Hash Functions (ISO 29192-5)
  - PHOTON حجم المخرجات 80-بت أو 128-بت أو 160-بت أو 224 -بت أو 256-بت.
  - SPONGENT حجم المخرجات 88-بت أو 128-بت أو 160-بت أو 224-بت أو 256 -بت.
  - Lesamnta-LW حجم المخرجات 256-بت.
- رموز توثيق الرسائل Message Authentication Code (MAC) (ISO 29192-6)
  - Tsudik's keymode.
  - Chaskey12، طول المفتاح 128-بت.

٣ تصاميم التشفير
Cryptographic Schemes

٣,١ طرق عمليات التشفير الكتلية Block Cipher Modes of Operation

التصاميم المقبولة:

- Counter Mode (CTR) كما في NIST SP800-38A.
- Cipher Block Chaining (CBC) كما في NIST SP800-38A.
- XEX Tweakable Block Cipher with Ciphertext Stealing (XTS-AES) كما في NIST SP800-38E.
- Output Feedback (OFB) كما في NIST SP800-38A.
- Cipher Feedback (CFB) كما في NIST SP800-38A.

ملاحظات عامة:

- CBC مقبول فقط للمستوى الأساسي.

٣,٢ رموز توثيق الرسائل Message Authentication Codes (MAC)

التصاميم المقبولة:

- Cipher-based MAC (CMAC) كما في NIST SP 800-38B
  - لا يزيد استخدام المفتاح الواحد لأكثر من 2^{48} رسالة.
  - تستخدم فقط في التطبيقات التي لا يستطيع أي طرف معرفة تشفير سلسلة الأصفار All-0 String.
  - أن يكون طول الوسم Tag على الأقل 96 بت مع مفاتيح توثيق آمنة.
- Hash-based MAC (HMAC) كما في FIPS PUB 198-1
  - أن يكون طول الوسم Tag على الأقل 96 بت مع مفاتيح توثيق آمنة.
  - أن تستخدم مع SHA-2 و SHA-3 (كما تم ذكره في القسم الفرعي ٢,٣).

٣,٣ التشفير والتوثيق باستخدام البيانات المرتبطة
Authenticated Encryption with Associated Data (AEAD)

التصاميم المقبولة:

- Galois Counter Mode (GCM) كما في NIST SP 800-38D
  - طول الرقم الابتدائي Nonce على الأقل 96 بت.
  - أن يكون متجه التهيئة (IV) فريدًا unique خلال فترة تغيير المفتاح.
  - من غير المسموح استخدام وسم توثيق Authentication Tag قصير.
- Counter with CBC-MAC (CCM) كما في NIST SP 800-38C.

٣,٤ دوال حماية المفاتيح Key Wrap Functions

التصاميم المقبولة:

- Key Wrap (KW) كما في NIST SP 800-38 F.
- Key Wrap with Padding (KWP) كما في NIST SP 800-38 F.

٣,٥ دوال اشتقاق المفاتيح Key Derivation Functions (KDF)

التصاميم المقبولة:

- RFC 5869 (HKDF)[4]
- IKE-v2-KDF[4]
- TLS-v1.2-KDF[4]
- X9.63-KDF[4]

ويجب أن تكون متوافقة مع التالي:

- NIST-800-56 A/B KDF (Single Step)[4].
- NIST-800-56 C KDF (Extract-then-expand)[4].
- NIST-800-108[4].

٣,٦ الاتفاق على المفاتيح ونقلها Key Agreement and Key Transport

٣,٦,١ التصاميم المتماثلة Symmetric Schemes

التصاميم المقبولة للاتفاق على المفاتيح:

- يتحقق الاتفاق على المفاتيح باستخدام التصاميم المتماثلة فقط بالاعتماد على بيانات سرية مشتركة طويلة المدى.

التصاميم المقبولة لنقل المفاتيح:

- يمكن استخدام جميع أساسيات وتصاميم التشفير المتماثلة بحسب ما ورد في القسم ٢ والقسم ٣.
- الجمع بين تصاميم التشفير والتوثيق باستخدام رموز توثيق الرسائل (MAC) بطريقة التشفير ثم التوثيق Encrypt-then-MAC mode (حسب ما ورد في القسم ٢ والقسم ٣).

٣,٦,٢ التصاميم غير المتماثلة Asymmetric Schemes

التصاميم المقبولة:

- Diffie-Hellman (DH) كما في RFC 3526
  - طول المفتاح 3072 بت على الأقل للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.

[4] European Commission, "eCrypt Algorithms, Key Size and Protocols Report," *in eCrypt Algorithms*, Key Size and Protocols Report, 2018.

- Elliptic Curve Diffie-Hellman (ECDH) كما في NIST SP 800-56A
  - طول المفتاح من 256-بت إلى 384-بت للمستوى الأساسي.
  - طول المفتاح 512-بت أو باستخدام المنحنى Curve448 للمستوى المتقدم.
  - مع تمكين خاصية السرية للأمام Forward Secrecy وتطبيق إنشاء المفاتيح الموثقة Authenticated Key Establishment.
- RSA Key Establishment (NIST 800-56B)
  - طول المفتاح 3072 بت على الأقل للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.

٣,٧ تصاميم التشفير الهجينة Hybrid Encryption Schemes

التصاميم المقبولة:

- Elliptic Curve Integrated Encryption Scheme (ECIES)
  - للمستوى الأساسي والمستوى المتقدم.
- Discrete Logarithm Integrated Encryption Scheme (DLIES)
  - للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.
- RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP) كما في PKCS #1 v2.1. RSA
  - للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.

٣,٨ تواقيع المفاتيح العامة Public Key Signatures

التصاميم المقبولة:

- Digital Signature Algorithm (DSA) كما في FIPS PUB 186-4
  - طول المفتاح 3072 بت على الأقل للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.
- Elliptical Curve Digital Signature Algorithm (ECDSA) كما في FIPS PUB 186-4
  - طول المفتاح من 256-بت إلى 384-بت للمستوى الأساسي.
  - طول المفتاح 512-بت أو باستخدام المنحنى Curve448 للمستوى المتقدم.
  - خوارزميات توثيق الرسائل المقبولة تعتمد بشكل أساسي على الأنظمة وحالات الاستخدام.

- RSA-PSS و RSA-DS2 [5,6].
  - طول المفتاح 3072 بت على الأقل للمستوى الأساسي.
  - غير مقبول للمستوى المتقدم.
- Merkle
  - يجب استخدام دوال الاختزال Hash Functions المقبولة في القسم ٢.
  - يجب أن يكون مولد الأعداد شبه العشوائية Pseudo-Random مبني باستخدام HMAC بناءً على دوال الاختزال المستخدمة.

[5] PKCS, "RSA Cryptographic Standard. Version 2.2," 2012.

[6] ISO, "ISO/IEC 9796-2-2010. Information technology - Security techniques - Digital Signature Schemes. Part 2: Integer Factorization based mechanisms.," 2010.

٤ بروتوكولات التشفير الشائعة
Commonly Used Cryptographic Protocols

يستعرض هذا القسم المتطلبات الفنية المقبولة لقائمة من بروتوكولات التشفير الشائعة الاستخدام. يجب الأخذ في الاعتبار أن أي بروتوكول غير مدرج هنا يجب أن تطبق عليه المتطلبات المذكورة في القسم ٢ والقسم ٣. بالإضافة إلى أن الإصدارات الجديدة في المستقبل للبروتوكولات المدرجة أدناه يجب أن تطبق عليها أيضا المتطلبات المذكورة في القسم ٢ والقسم ٣.

٤,١ بروتوكول الإنترنت الآمن IP Security (IPsec)

المتطلبات المقبولة:

بالنسبة للتوثيق Authentication، يجب استخدام حقل التوثيق Authentication Header (AH) وتغليف البيانات الآمن Encapsulating Security Payload (ESP) مع تصاميم التوثيق MAC التالية:

- HMAC-SHA2-384 أو HMAC-SHA3-256 أو HMAC-SHA3-384 للمستوى الأساسي.
- HMAC-SHA3-512 للمستوى المتقدم.

بالنسبة للسرية Confidentiality، يجب استخدام تغليف البيانات الآمن (ESP) مع أحد تصاميم التوثيق MAC أعلاه وأحد خوارزميات التشفير التالية[7]:

- AES-CTR
- CAMELLIA-CTR

كخيار آخر، يمكن استخدام التشفير والتوثيق باستخدام أحد الطرق التالية[7]:

- AES-CCM_*، وترمز * إلى الحجم بالبايت لقيمة التحقق من السلامة Integrity Check Value (ICV)
  - المقبول 12 أو 16 بايت.
- CAMELLIA-CCM_*، وترمز * إلى الحجم بالبايت لقيمة التحقق من السلامة (ICV)
  - المقبول 12 أو 16 بايت.
- AES-GCM_*، وترمز * إلى الحجم بالبايت لقيمة التحقق من السلامة (ICV)
  - المقبول 12 أو 16 بايت.

٤,٢ بروتوكول طبقة النقل الآمنة Transport Layer Security (TLS)

الإصدارات المقبولة:

- يُقبل استخدام TLS 1.2 مع أساسيات وتصاميم التشفير المقبولة حسب المتطلبات في القسم ٢ والقسم ٣ لضمان التوافق وتطبيق إعدادات لا تسمح بخفض درجة القوة[8] .
- تطبيق استخدام TLS 1.3 سيستغرق بعض الوقت، وينصح باعتماده للتطبيقات المستقبلية.

[7] European Union Agency for Network and Information Security "Study on cryptographic protocols," 2014.

[8] E. Ronen, "The 9 Lives of Bleichenbacher's CAT. New Cache Attacks on TLS Implementations.," 2018.

المتطلبات المقبولة في TLS 1.2:

- TLS_*1_*2_WITH_AES_128_CCM و TLS_*1_*2_WITH_AES_128_CCM_8 و TLS_*1_*2_WITH_Camellia_256_GCM_SHA-384 و TLS_*3_*4_WITH_AES_256_GCM_SHA-384 للمستوى الأساسي.
- TLS_*3_*4_WITH_AES_256_CCM و TLS_*3_*4_WITH_AES_256_CCM_8 للمستوى المتقدم.

باعتبار أن:

*1 تصميم اتفاق المفاتيح: ECDH أو ECDHE أو DH أو DHE.

*2 تصميم التوقيع: EC_DSA أو RSA أو DSS.

*3 تصميم اتفاق المفاتيح: ECDH أو ECDHE.

*4 تصميم التوقيع: EC_DSA.

المتطلبات المقبولة في TLS 1.3:

- TLS_AES_256_GCM_SHA384 للمستوى الأساسي والمستوى المتقدم [8].

٤,٣ بروتوكول نظام اسم النطاق الآمن DOMAIN NAME SYSTEM SECURITY (DNSSEC)

المتطلبات المقبولة لتوقيع بيانات المنطقة Zone Data Signing:

- ECDSA_P384_SHA-384 للمستوى الأساسي والمستوى المتقدم[9,10].

المتطلبات المقبولة لتوثيق الرسائل Message Authentication:

- HMAC_SHA-384 للمستوى الأساسي.
- HMAC_SHA-512 للمستوى المتقدم[9].

٤,٤ بروتوكول الاتصال الآمن عن بعد Secure Shell (SSH)

الإصدارات المقبولة: SSH-2.

المتطلبات المقبولة:

- AEAD_AES_128_GCM للمستوى الأساسي.
- AEAD_AES_256_GCM للمستوى المتقدم.

٤,٥ بلوتوث Bluetooth

الإصدارات المقبولة: Bluetooth 4.1 أو أعلى.

المتطلبات المقبولة (NIST SP 800-121r2):

- استخدام وضع الأمان ٤ (Security Mode 4) ، المستوى ٤ (Level 4) مع مفتاح اتصال موثق وباستخدام قنوات اتصال آمنة.

[9] في حين أن SHA3 512-بت لم يتم تنفيذها لهذا البروتوكول، تعتبر هذه حالة استثنائية للمستوى المتقدم، وكذلك HMAC-SHA-512 غير معرض لهجمات Length Extension Attacks.

[10] في حين أنECC 512-بت لم يتم تنفيذها لهذا البروتوكول، تعتبر هذه حالة استثنائية للمستوى المتقدم.

- استخدام خوارزمية التشفير AES-CCM.
- استخدام خاصية الاتصال الآمن مع ECC P-256 لإنشاء مفتاح الاتصال.
- استخدم وضع أمان التشفير ٣ (Encryption Mode 3) مع تشفير جميع المراسلات (Encrypt All Traffic).
- بالنسبة للبلوتوث منخفض الطاقة Bluetooth Low Energy (BLE) يجب استخدام إصدار Bluetooth 4.2 أو أعلى، مع وضع أمان الطاقة المنخفضة ١ (Low Energy Security Mode 1) المستوى ٤ (Level 4).

ملاحظات عامة:

- يجب استخدام أقوى أوضاع الأمان المتاحة في أجهزة البلوتوث.

٤,٦ نظام الاتصالات المتنقلة العالمية (UMTS) / الجيل الرابع (LTE) / الجيل الخامس (5G)

المتطلبات المقبولة:

- بالنسبة لنظام الاتصالات المتنقلة العالمية (UMTS) يجب استخدام 128-UEA1 مع 128-UIA1.
- بالنسبة للجيل الرابع (LTE) يجب استخدام 128-EEA2 مع 128-EIA2.
- بالنسبة للجيل الخامس (5G) يجب استخدام أو 128-NEA2 مع 128-NIA2.
- يمكن استخدام EIA0 و NIA0 في الحالات الاستثنائية للمكالمات الطارئة غير الموثقة Unauthenticated في وضع الخدمة المحدود Limited Service Mode.
- يجب استخدام أساسيات وتصاميم التشفير المذكورة في القسم ٢ والقسم ٣ فقط. ولكن كاستثناء من المقبول استخدام خوارزمية KASUMI وECIES Profile A و ECIES Profile B حيث تُقبل كاستثناء خاص لأنظمة 3GPP.

٤,٧ الوصول الآمن للشبكة اللاسلكية WPA (Wi-Fi Protected Access)

الإصدارات المقبولة:

- WPA3-Enterprise

ملاحظات عامة:

- WPA3-Enterprise هو الإصدار المقبول فقط ويجب تطبيقه عند توفره.
- استخدام بروتوكول آمن بما يتوافق مع أساسيات وتصاميم التشفيرحسب القسم ٢ و القسم ٣.

٤,٨ بروتوكول كيربيروس Kerberos Protocol

المتطلبات المقبولة:

- CAMELLIA128-CTS-CMAC و AES256-CTS-HMAC-SHA384 للمستوى الأساسي.
- CAMELLIA256-CTS-CMAC للمستوى المتقدم.

0 البنية التحتية للمفاتيح العامة Public Key Infrastructure (PKI)

0,1 خوارزميات الشهادات Algorithms for Certificates

الخوارزميات المقبولة للشهادات الجذرية Root CA Certificates:

- RSA
  - طول المفتاح 4096 بت على الأقل.
- ECC
  - NIST P-384 و NIST P-521 و Curve448 و BrainpoolP384r1 و BrainpoolP512r1.

الخوارزميات المقبولة للشهادات المتوسطة وشهادات المستخدم النهائي Intermediate and End User Certificates:

- RSA
  - طول المفتاح 3072 بت على الأقل.
- ECC
  - NIST P-256 و NIST P-384 و NIST P-521 و Curve25519 و Curve448 و BrainpoolP256r1 و BrainpoolP384r1 و BrainpoolP512r1.

ملاحظات عامة:

- يجب أن تتوافق الشهادات Certificates وقائمة الشهادات الملغية Certificate Revocation Lists (CRLs) وقائمة الهيئات الملغية Authority Revocation Lists (ARLs) مع X.509 PKI (RCF 5280).
- يجب استخدام دوال الاختزال Hash Functions المقبولة في القسم ٢.
- يجب أن يتوافق مستوى قوة خوارزميات المفاتيح غير التماثلية Asymmetric Key Algorithms مع مستوى قوة خوارزميات الاختزال Hash Algorithms.

0,2 صلاحية الشهادات Validity of the Certificates

فترة صلاحية الشهادات الجذرية Root CA Certificates:

- ٢٠ سنة كحد أقصى[11].

فترة صلاحية شهادات هيئات الشهادات المتوسطة والثانوية والمانحة Intermediate CA, Subordinate CA and Issuing CA:

- ١٠ سنوات كحد أقصى[11].

فترة صلاحية شهادات المستخدم النهائي End User Certificate:

- ٥ سنوات كحد أقصى للمستوى الأساسي[11].
- ٣ سنوات كحد أقصى للمستوى المتقدم[11].

[11] NIST, "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Federal Public Key Infrastructure Policy Authority," *NIST*, 2015

٦ إدارة دورة المفاتيح
Key Lifecycle Management (KLM)

٦,١ حماية المفاتيح وصلاحيتها Key Protection and Lifetime

حماية المفاتيح وصلاحيتها المقبولة:

- استخدام أجهزة وحدات التشفير Hardware Cryptographic Modules
  - يجب أن تكون المفاتيح الخاصة Private Keys صالحة لمدة لاتزيد عن ٥ سنوات (لا يحد هذا من فترة صلاحية شهادات هيئات الشهادات CA Certificates) للمستوى الأساسي[12].
  - يجب أن تكون المفاتيح الخاصة Private Keys صالحة لمدة لاتزيد عن ٣ سنوات (لا يحد هذا من فترة صلاحية شهادات هيئات الشهادات) للمستوى المتقدم [12].
- استخدام برمجيات وحدات التشفير Software Cryptographic Modules
  - لا يسمح أن تكون المفاتيح الخاصة Private Keys صالحة لأكثر من سنتين للمستوى الأساسي [12].
  - غير مقبول للمستوى المتقدم.

٦,٢ عمليات إدارة دورة المفاتيح KLM Processes

يوضح الجدول ١ أهم المتطلبات التي يجب الالتزام بها لكل عملية ضمن دورة حياة المفاتيح منذ إنشائها وحتى إتلافها.

جدول ١ – متطلبات عمليات إدارة دورة المفاتيح KLM Processes Requirements

العملية	المتطلبات
إنشاء المفاتيح Key Generation	• يجب أن تكون المفاتيح (السرية والخاصة Secret and Private) غير معرضة للتنبؤ Prediction أو الانحياز Bias. • يجب عدم استخدام المفاتيح الضعيفة. • تتطلب المفاتيح الخاصة والعامة Private and public keys توليد أعداد أولية مع خصائص رياضية إضافية.
تسجيل/تصديق المفاتيح Key Registration /Certification	• يجب أن يكون المفتاح مرتبطًا بصاحبه (المستخدم) مع وجود شهادة Certificate بذلك. • يجب توزيع الشهادات الجذرية Root Certificates على الأطراف المعتمدة. • يجب استخدام هيئات شهادات موثوقة Trusted CA.

[12] E. Barker, "Recommendation for Key Management: Part 1 - General," NIST, NIST Special Publication 800-57 Part 1 Revision 5, May 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5.

توزيع المفاتيح وتثبيتها **Key Distribution and Installation**	• يجب توزيع المفاتيح على مستخدميها بطريقة آمنة وأن تكون تحت تحكم المستخدم. • يجب نقل المفاتيح بطريقة آمنة وذلك بحماية سريتها Confidentiality وموثوقيتها Authenticity. • يجب تثبيت وتخزين جميع نسخ المفاتيح بأمان. • يجب نقل المفاتيح العامة Public Keys ويجب حماية موثوقيتها Authenticity باستخدام الشهادات Certificates. • يجب حماية المفاتيح الخاصة Private Keys ومنح الصلاحيات من قبل المالك أو الطرف الثالث أو هيئة الشهادات CA.
استخدام المفاتيح **Key Use**	• يجب حماية المفاتيح ضد الاستخدام غير المصرح به منذ إنشائها وحتى إتلافها. • يجب حماية المفاتيح ضد إساءة الاستخدام من مُلاك المفاتيح أنفسهم وذلك باستخدام مخزن للمفاتيح Key Storage على جهاز أو برنامج آمن Secure Hardware or Secure Software (مع فحوصات منح الصلاحيات Authorization Checks).
تخزين المفاتيح **Key Storage**	• يجب على الجهات أن تحتفظ بنسخ احتياطية آمنة للمفاتيح (للاستخدام الداخلي أو لتطبيق القانون for internal or law enforcement use) في حال أن خوارزميات التشفير لاتزال مدعومة. • يجب أن تكون المفاتيح المستخدمة لغرض عدم الإنكار Non-repudiation تحت التحكم الحصري من قبل المستخدم.
إلغاء المفاتيح والتحقق من صحتها **Key Revocation/ Validation**	• في الأنظمة الموزعة يجب اعتماد تدابير خاصة مثل الاعتماد على إصدارات محدثة لقائمة الشهادات الملغية Certificate Revocation List (CRL) وبروتوكول حالة الشهادة عبر الإنترنت Online Certificate Status Protocol (OCSP) لتفادي استخدام مفاتيح منتهية الصلاحية. • يجب التحقق من صحة المفاتيح عن طريق التأكد من خوادم قائمة الشهادات الملغية (CRL) وبروتوكول حالة الشهادة عبر الإنترنت (OCSP).
أرشفة المفاتيح **Key Archive**	• يجب تأمين عملية أرشفة المفاتيح لضمان سريتها للحفاظ على سرية المعلومات المشفرة. • يجب أرشفة المفاتيح منتهية الصلاحية Expired Keys لضمان الوصول إلى البيانات القديمة .في حال أن خوارزميات التشفير لاتزال مدعومة. • يجب أن تتبع أنظمة الأرشفة فترات الاحتفاظ Retention Periods وفقًا للتنظيمات ذات العلاقة.

إتلاف المفاتيح **Key Destruction**	• عند انتهاء فترة حياة المفتاح ولم تكن هناك أي حاجة لتخزينه أو أرشفته، يجب إزالته من الجهاز عن طريق عملية حذف آمنة. • يجب تنقية أنظمة تخزين الوسائط التي يتم حفظ المفاتيح فيها عند الإتلاف حسب الإجراءات الواردة في NIST SP 800-88r1 أو NSA/CSS Storage.
المحاسبة على المفاتيح **Key Accounting**	• يجب أن يكون هناك محاسبة على جميع المفاتيح غير التماثلية Asymmetric Keys. • تجب مراقبة استخدام المفاتيح غير التماثلية Asymmetric Keys. • يجب أن يكون هناك محاسبة على استخدام المفاتيح.

٧ الملحقات

٧,١ توليد الأعداد شبه العشوائية Pseudo Random Number Generation (PRNG)

توليد الأعداد شبه العشوائية عامل أساسي في العديد من أنظمة التشفير، ويشمل إنشاء المفاتيح المتماثلة Symmetric Keys وزوج المفاتيح غير المتماثلة Asymmetric Key-pairs[13].

يُمنع استخدام دوال مكتبات البرامج التابعة للغات البرمجة مثل `random()` في توليد الأعداد شبه العشوائية، لأن هذه الدوال تميل إلى الاعتماد على مولدات خطية تطابقية Linear Congruential Generators (LCG) ضعيفة. وإنما يلزم استخدام أدوات لتوليد الأعداد شبه العشوائية (PRNG) تكون متخصصة لتطبيقات التشفير، ويجب أن يتم اختبارها من خلال حزم الاختبارات المناسبة، مثل اختبارات العشوائية من المعهد الوطني للمعايير والتقنية (NIST)[14] وحزمة اختبارات Dieharder[15].

لمزيد من المعلومات عن متطلبات مولد الأعداد شبه العشوائية، يمكن الرجوع للمعايير العالمية ومنها: "Random variate generation methods" ISO 28640:2010 و NIST SP 80090-A "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

٧,٢ التشفير ما بعد الحوسبة الكمية Post-Quantum Cryptography

تهدد الأنظمة الحاسوبية الكمية أنظمة التشفير التقليدية. حيث أنه سيتم كسر العديد من أنظمة التشفير شائعة الاستخدام عند توفر الأنظمة الحاسوبية الكمية بالقدرة الكافية من البتات الكمية qubits. وسيكون معظم التأثير على أنظمة التشفير ذات المفاتيح العامة مثل RSA[16] و DSA و ECDSA.

على الرغم من أنه غير معلوم حتى الآن توفر الأنظمة الحاسوبية الكمية بالعدد الكافي من البتات الكمية qubits أو استخدامها تجاريًا ، إلا أن خطرها على سرية البيانات كبير، هذا الخطر معترف به عالميا لذلك من المهم جدا اعتماد خوارزميات التشفير ما بعد الحوسبة الكمية.

ولكن لا تزال المعايير الدولية الخاصة بالتشفير لما بعد الحوسبة الكمية غير متوفرة وغير معتمدة، ومن المتوقع أن يتم إصدارها خلال الثلاث سنوات القادمة. وسيتم اعتماد خوارزميات التشفير لما بعد

[13] European Commission, "eCrypt Algorithms, Key Size and Protocols Report," in *eCrypt Algorithms*, Key Size and Protocols Report, 2018.

[14] NIST, "Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST*, 2010.

[15] R. Brown, "Robert G. Brown's General Tools Page," 2019. [Online]. Available: http://webhome.phy.duke.edu/~rgb/General/dieharder.php.

[16] NIST, "NISTIR 8105. Report on Post-Quantum Cryptography," 2016.

الحوسبة الكمية في الإصدارات القادمة من المعايير الوطنية للتشفير.

٧,٣ هجمات القنوات الجانبية Side-channel Attacks

تعتمد الهجمات على القنوات الجانبية لأنظمة التشفير على نتائج القياسات المادية (الفيزيائية) للنظام، مثل استهلاك الطاقة والانبعاث الكهرومغناطيسي واستهلاك الوقت، من أجل الوصول للبيانات الحساسة [17] . حيث يمكن تنفيذ هجمات من قبل أعداء غير نشيطين ويعملون عن بُعد مما يزيد من صعوبة اكتشافهم، وقد يؤدي إلى تسرب هام وغير ملحوظ للبيانات.

ولمنع هذا النوع من الهجمات وللحد من تسرب المعلومات يجب التأكد من ضعف إشارة القنوات الجانبية بحيث تكون نسبة الإشارة إلى الضوضاء signal-to-noise ratio منخفضة قدر الإمكان. علاوة على ذلك، يجب التأكد من أن المعلومات المتسربة من القنوات الجانبية ليست مهمة وغير مفيدة للمهاجمين [18]. على سبيل المثال ، إزالة أي ارتباط بين التمثيل الثنائي للمفتاح السري وإشارات القناة الجانبية ، أي باستخدم عمليات وهمية لإخفاء أي ارتباط محتمل.

التدابير اللازمة لتقليل مخاطر هجمات القنوات الجانبية[19]:

- إجراء عمليات التشفير داخل مكونات الأجهزة (العتاد) المعتمدة، على سبيل المثال: لحماية المفاتيح السرية والخاصة.
- إجراء تحليل شامل لآثار هذه القنوات الجانبية على مكونات الأجهزة (العتاد) المعتمدة في مختبر متخصص أثناء عملية التطوير.
- حماية جميع البيانات المشفرة باستخدام رموز توثيق الرسائل (MAC). كما يجب التحقق من موثوقية البيانات المشفرة قبل إجراء أية عمليات تشفير أخرى. كما يجب الامتناع عن إجراء أي معالجة أخرى للبيانات المشفرة غير الموثوقة.

هجمات القنوات الجانبية تشمل مجموعة واسعة من التهديدات ذات الصلة، وعليه ينبغي مراجعة التهديدات ذات الصلة من أجل التنفيذ الآمن والسليم لأنظمة التشفير.

[17] P. C. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in *Differential power analysis*, 2011.

[18] A. Vega, P. Bose and A. Buyuktosunoglu, "Rugged Embedded Systems: Computing in Harsh Environments", *Morgan Kaufmann*, 2017.

[19] BSI, "Cryptographic Mechanisms: Recommendations and Key Lengths", BSI - Technical Guideline, 2020

٧,٤ تعريفات

جدول ٢- مصطلحات وتعريفات [20]

المصطلح	التعريف
Asymmetric Algorithm **خوارزمية غير متماثلة**	خوارزمية تشفير تستخدم مفتاح لعملية التشفير ومفتاح آخر لفك التشفير. يسمى المفتاحان المفتاح الخاص والمفتاح العام.
Authentication **التوثيق**	التحقق من هوية المستخدم أو العملية أو الجهاز، غالبًا ما تكون شرط مسبق للسماح بالوصول إلى موارد النظام.
Authenticity **الموثوقية**	خاصية الأصالة مع القدرة على التحقق منها والثقة بها.
Block Cipher Algorithm **خوارزمية التشفير الكتلية**	طريقة تشفير المفتاح المتماثل والتي تقسم البيانات إلى مجموعات أو كتل، ثم تقوم بتشفير كل واحدة على حدة.
Certificate **شهادة**	مجموعة من البيانات التي تحدد بصفة فريدة المفتاح العمومي للكيان والمعلومات الأخرى التي يتم توقيعها رقميًا من قبل هيئات الشهادات (أطراف موثوقة)، وبهذا الشكل يتم ربط المفتاح العمومي بالمالك.
Certificate Revocation List (CRL) **قائمة الشهادات الملغية**	قائمة الشهادات الملغية المعلنة من هيئة الشهادات CA.
Certification Authority (CA) **هيئة الشهادات**	كيان موثوق مسؤول عن إصدار وإلغاء شهادات المفاتيح العامة.
Collision **التعارض**	مدخلان متمايزان عن بعضهما البعض أو أكثر لهما نفس المخرج.
Confidentiality **السرية**	خاصية منع إتاحة المعلومات أو الكشف عنها للأفراد أو الكيانات أو العمليات غير المصرح لها.

[20] مصطلحات المعهد الوطني للمعايير والتقنية NIST Glossary (إلا ما يتم توضيحه بالنسبة لمصطلح محدد).

Cryptographic Primitive **أساسيات التشفير**	خوارزمية تشفير منخفضة المستوى تستخدم كوحدة بناء أساسية لخوارزميات التشفير ذات المستويات الأعلى منها.
Cryptography **التشفير**	مبادئ ووسائل وطرق لتطبيق خوارزميات تحويل البيانات لأغراض أمنية تشمل السلامة والسرية والتوثيق، والموثوقية، ومنع الإنكار.
Cybersecurity **الأمن السيبراني**	حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك [21] .
Decryption **فك التشفير**	عملية تحويل البيانات المشفرة إلى البيانات الأصلية باستخدام أحد خوارزميات تقنيات التشفير والمفتاح الخاص بذلك.
Digital Signature **التوقيع الإلكتروني**	هو ناتج تحويل تشفيري للبيانات والذي يتيح عند تنفيذه بالشكل المناسب خواص التوثق وسلامة البيانات، ومنع إنكار الطرف المُوقِّع.
Digital Signature Algorithm (DSA) **خوارزمية التوقيع الإلكتروني**	خوارزمية يستخدمها المُوقِّع لإنشاء توقيع رقمي على البيانات، ويستخدمه المدقق للحصول على توكيد مصدر المعلومات الموقعة وسلامتها.
Elliptic Curve Cryptography (ECC) **التشفير بالمنحنى الإهليجي**	طرق تشفير بالمفاتيح العامة تستخدم عمليات في مجموعة منحنى إهليجي.
Encryption **عملية التشفير**	عملية تحويل بيانات أصلية إلى بيانات مشفرة باستخدام أحد خوارزميات تقنيات التشفير والمفتاح الخاص بذلك.
Hash Function **دالة الاختزال**	دالة تقوم بتحويل سلسلة أرقام ثنائية ذات طول عشوائي إلى سلسلة أرقام ثنائية ذات طول ثابت. غالبًا ما يستحيل إعادة هذا المخرج إلى أصله، ويمثل هذا المخرج صورة مختصرة للمدخلات.

[21] تنظيم الهيئة الوطنية للأمن السيبراني الصادر بالأمر الملكي الكريم رقم ٦٨٠١ ، وتاريخ ١١ / ٢/ ١٤٣٩هـ

Hash-based MAC (HMAC) رموز توثيق الرسائل المبنية على دوال الاختزال	رموز لتوثيق الرسائل باستخدام دالة اختزال مقبولة ومفتاح.
Hybrid Encryption التشفير الهجين	تطبيق للتشفير يجمع بين خوارزميتي تشفير أو أكثر، وعلى وجه التحديد الدمج بين التشفير المتماثل وغير المتماثل [22].
Initialization Vector (IV) متجه التهيئة	متجه عام معلوم يستخدم كمدخل لتهيئة خوارزمية التشفير لرفع مستوى الأمن ودعم التزامن.
Integrity السلامة	خاصية عدم تغيير البيانات بصفة غير مصرح بها منذ إنشائها أو خلال نقلها أو تخزينها.
Integrity Check Value (ICV) قيمة التحقق من السلامة	ناتج عملية جمع خاصة يمكن من خلاله اكتشاف التعديلات على نظام معلوماتي.
Kerberos Protocol بروتوكول كيربيروس	نظام توثيق تم تطويره لتمكين طرفين من تبادل المعلومات الخاصة عبر شبكة عامة.
Key Agreement الاتفاق على المفاتيح	إجراء لإنشاء المفاتيح بحيث تكون مادة المفاتيح الناتجة تتولد عن دالة تعالج معلومات أسهم بها اثنان أو أكثر من المشاركين، بحيث لا يمكن لأي طرف منهم تحديد قيمة مادة المفاتيح باستقلال عن مساهمة الأطراف الاخرى.
Key Archive أرشفة المفاتيح	وظيفة في دورة المفاتيح عبارة عن مستودع للتخزين طويل الأجل لمكونات المفاتيح.
Key Derivation Function (KDF) دالة اشتقاق المفاتيح	هي العملية التي يتم من خلالها اشتقاق مفتاح أو أكثر إما من مفتاح تمت مشاركته مسبقًا أو من معلومات سرية وأخرى مشتركة.
Key Destruction إتلاف المفاتيح	عملية إزالة جميع آثار مادة المفاتيح بحيث لا يمكن استردادها بأي وسيلة مادية أو إلكترونية.

[22] SANS Glossary

Key Distribution **توزيع المفاتيح**	انظر إلى "نقل المفاتيح Key Transport".
Key Exchange **تبادل المفاتيح**	عملية تبادل المفاتيح العامة لتأسيس اتصالات آمنة.
Key Generation **إنشاء المفاتيح**	عملية توليد مفاتيح للتشفير.
Key Lifecycle Management (KLM) **دورة إدارة المفاتيح**	الأنشطة التي تشمل التعامل مع مفاتيح التشفير ومعاملات الأمان ذات الصلة (مثل متجهات التهيئة) خلال دورة المفاتيح، ويشمل ذلك الإنشاء والتخزين والتأسيس والإدخال والإخراج والاستخدام والإتلاف.
Key Registration / Certification **تسجيل المفاتيح / إصدار الشهادة**	وظيفة ضمن دورة حياة المفتاح؛ تتمثل بعملية التسجيل الرسمي لمكونات المفتاح بواسطة هيئات الشهادات.
Key Revocation **إلغاء المفاتيح**	وظيفة ضمن دورة حياة المفتاح؛ هي عملية يتم بموجبها إشعار الكيانات المتأثرة بأن المفتاح وما يتعلق به من مكونات يجب إزالته من الاستخدام التشغيلي قبل نهاية فترة التشفير المحددة لمكونات هذا المفتاح.
Key Transport **نقل المفاتيح**	إجراء لتأسيس المفتاح حيث تقوم أحد الجهات بنقل وإيصال المفتاح إلى جهة أخرى.
Key Wrap **تغليف المفاتيح (حماية المفاتيح)**	طريقة لتشفير المفاتيح (تشمل معلومات السلامة) والتي توفر كل من السرية والسلامة وذلك باستخدام خوارزمية مفاتيح متماثلة.
Lightweight Crypto **التشفير الخفيف**	فئة فرعية في مجال التشفير تهدف إلى توفير حلول أمنية للأجهزة محدودة الموارد.
Message Authentication Code (MAC) **رموز توثيق الرسائل**	مجموع اختباري تشفيري للبيانات والذي يستخدم مفتاحًا متماثلاً للكشف عن التعديلات المقصودة وغير المقصودة على البيانات.كما توفر رموز توثيق الرسائل خاصية الموثوقية والسلامة.

Non-repudiation **عدم الإنكار**	خدمة تستخدم التوقيع الرقمي للتحقق من أن كيان محدد قد وقع فعليًا على رسالة محددة حيث لا يمكنه نفي ذلك.
Private Key **مفتاح خاص**	في الخوارزمية غير المتماثلة يتم استخدام المفتاح الخاص للتوقيع الرقمي وأيضا لفك تشفير البيانات، ويجب أن يبقى سريًا.
Public Key **مفتاح عام**	في الخوارزمية غير المتماثلة يتم استخدام المفتاح العام للتحقق من التوقيع الرقمي وأيضا لتشفير البيانات، ويكون معروفاً للعموم.
Public Key Infrastructure (PKI) **البنية التحتية للمفاتيح العامة**	إطار تم إنشاؤه لإصدار شهادات المفاتيح العامة والحفاظ عليها وإلغائها.
RSA	خوارزمية غير متماثلة يتم استخدامها لإنشاء المفاتيح وتوليد التوقيع الرقمي والتحقق منه.
Stream Cipher Algorithm **خوارزمية التشفير الانسيابية**	طريقة تشفير المفتاح المتماثل حيث يتم تشفير كل رقم ثنائي أو كلمة ثنائية واحدة تلو الأخرى بأرقام ثنائية شبه عشوائية (المفتاح الانسيابي) باستخدام بيانات داخلية متغيرة مع الوقت لإنتاج رقم ثنائي أو كلمة ثنائية مشفرة.
Strong Primes **أعداد أولية قوية**	في التشفير يتم تعريف الأعداد الأولية القوية على أنها أعداد أولية يصعب تحليل نواتج ضربها إلى مكوناتها أو عواملها. وبصفة خاصة: الرقم الأولي p يعد قويا إذا تحقق فيه كل مما يلي: أ. $p - 1$ لديه عامل أولي كبير q و ب. $q - 1$ لديه عامل أولي كبير و ج. $p + 1$ لديه عامل أولي كبير.
Symmetric Algorithm **خوارزمية متماثلة**	خوارزمية تشفير تستخدم مفتاح سري واحد لكل من عمليتي التشفير وفك التشفير.

٧,٥ قائمة الاختصارات

جدول ٣ – قائمة الاختصارات

الاختصار	معناه
AEAD	Authenticated Encryption with Associated Data التشفير والتوثيق باستخدام البيانات المرتبطة
AES	Advanced Encryption Standard معيار التشفير المتقدم
AH	Authentication Header حقل التوثيق
ALIKE	Authenticated Lightweight Key Exchange تبادل المفاتيح الخفيفة والموثقة
ARLs	Authority Revocation Lists قوائم الهيئات الملغية
CA	Certificate Authority هيئة شهادات
CBC	Cipher Block Chaining كتل التشفير المتسلسلة
CCM	Counter with CBC-MAC عداد مقترن بكتل التشفير المتسلسلة لرموز توثيق الرسائل
CFB	Cipher Feedback التغذية الراجعة للتشفير
CMAC	Cipher-based Message Authentication Code رموز توثيق الرسائل المبنية على التشفير
CRLs	Certificate Revocation Lists قوائم الشهادات الملغية
CTR	Counter mode كتل التشفير باستخدام العداد
DH	Diffie-Hellman ديفي-هيلمان

DLIES	Discrete Logarithm Integrated Encryption Scheme تصاميم التشفير اللوغاريثمي المتكامل
DNSSEC	Domain Name System Security نظام اسم النطاق الآمن
DSA	Digital Signature Algorithm خوارزمية التوقيع الرقمي
ECC	Elliptic Curve Cryptography التشفير باستخدام المنحنى الإهليجي
ECDLP	Elliptic Curve Discrete Logarithm Problem مسألة المنحنى الإهليجي اللوغاريثمي المتقطع
ECDSA	Elliptical Curve Digital Signature Algorithm خوارزمية التوقيع الإلكتروني بالمنحنى الإهليجي
ECIES	Elliptic Curve Integrated Encryption Scheme تصاميم التشفير المدمجة بالمنحنى الإهليجي
EEA	EPS Encryption Algorithm خوارزمية التشفير لنظام الحزم المطور
EIA	EPS Integrity Algorithm خوارزمية السلامة لنظام الحزم المطور
EPS	Evolved Packet System نظام الحزم المطور
ESP	Encapsulating Security Payload تغليف البيانات الآمن
FIPS	Federal Information Processing Standards المعايير الفيدرالية لمعالجة المعلومات
GCM	Galois Counter Mode وضع عداد جالوا لرموز توثيق الرسائل
HKDF	Hash-based Key Derivation Function دالة اشتقاق المفاتيح المبنية على دالة الاختزال
HMAC	Hash-based Message Authentication Code رموز توثيق الرسائل المبنية على دالة الاختزال

ICV	Integrity Check Value قيمة التحقق من السلامة
IKE-v2	Internet Key Exchange version 2 الإصدار الثاني من نظام تبادل مفاتيح الإنترنت
IPsec	Internet Protocol Security بروتوكول الإنترنت الآمن
ISO/IEC	International Organization for Standardization/ The International Electrotechnical Commission المنظمة الدولية للتقييس/ اللجنة الكهروتقنية الدولية
IV	Initialization Vector متجه التهيئة
KDF	Key Derivation Functions دوال اشتقاق المفاتيح
KLM	Key Lifecycle Management إدارة دورة المفاتيح
KW	Key Wrap تغليف المفاتيح (حماية المفاتيح)
KWP	Key Wrap with Padding تغليف المفاتيح مع التعبئة
LTE	Long-Term Evolution بروتوكول التطور طويل الأمد (الجيل الرابع)
MAC	Message Authentication Code رموز توثيق الرسائل
NEA	NR Encryption Algorithm خوارزمية التشفير للراديو الجديد
NIA	NR Integrity Algorithm خوارزمية السلامة للراديو الجديد
NIST	National Institution of Standard and Technology المعهد الوطني للمعايير والتقنية
NR	New Radio الراديو الجديد

OCSP	Online Certificate Status Protocol بروتوكول حالة الشهادة عبر الإنترنت
OFB	Output Feedback التغذية الراجعة للمخرجات (أحد عمليات التشفير)
PKI	Public Key Infrastructure البنية التحتية للمفاتيح العامة
RSA	Algorithm developed by Rivest, Shamir and Adelman خوارزمية تم تطويرها من قبل ريفست وشامير وأدلمان
RSA-OAEP	RSA with Optimal Asymmetric Encryption Padding خوارزمية RSA مع التشفير غير التماثلي بالتعبئة الأفضل
SHA-2	Secure Hash Algorithm 2 الإصدار الثاني من خوارزمية الاختزال الآمن
SHA-3	Secure Hash Algorithm 3 الإصدار الثالث من خوارزمية الاختزال الآمن
SSH	Secure Shell الاتصال الآمن عن بعد
TLS	Transport Layer Security بروتوكول طبقة النقل الآمنة
UEA	UMTS Encryption Algorithm خوارزمية تشفير نظام الاتصالات المتنقلة العالمية
UIA	UMTS Integrity Algorithm خوارزمية سلامة نظام الاتصالات المتنقلة العالمية
UMTS	Universal Mobile Telecommunications System نظام الاتصالات المتنقلة العالمية
WPA	Wi-Fi Protected Access بروتوكول حماية الوصول إلى شبكات الواي فاي اللاسلكية

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority