الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

المعايير الوطنية للتشفير

National Cryptographic Standards

(NCS-2:2025)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

تنويه: لمواكبة المتغيرات المتسارعة بشأن تحديثات الوثائق الصادرة عن الهيئة الوطنية للأمن السيبراني، تود الهيئة الوطنية للأمن السيبراني التنويه على أهمية الاعتماد الدائم على نسخ الوثائق المنشورة في الموقع الإلكتروني للهيئة https://nca.gov.sa

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر (شخصي وسري للمستلم فقط)

المستلم لا يحق له مشاركة المعلومات مع أي فرد، سواء أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالي +مشدد

المستلم يمكنه مشاركة المعلومات في الجهة نفسها فحسب.

برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها فحسب أو من يتطلب الأمر منه اتخاذ إجراء يخص المعلومة من خارج الجهة، وذلك وفقًا لمبدأ الحاجة إلى المعرفة.

أخضر (مشاركة في نفس المجتمع)

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

شفاف (غير محدود)

المستلم يمكنه مشاركة المعلومات مع الجميع.

التحديثات والمراجعة

هذه النسخة من الوثيقة (NCS-2:2025) تحل محل النسخ السابقة (NCS-1:2020). تتولى الهيئة التحديث والمراجعة الدورية، لهذه الوثيقة؛ وذلك حسب المستجدات في مجالات التشفير، والمجالات ذات العلاقة. كما تتولى الهيئة، إعلان الإصدار المحدث من المعايير للعمل به.

نسخ الوثيقة

النسخة	سنة الإصدار	التحديثات
NCS - 1	٢٠٢٠	**النسخة الأولى**
NCS - 2	٢٠٢٥	**النسخة الثانية** **الملحق (ز) يوضح التحديثات**

قائمة المحتويات

قائمة الجداول

قائمة الأشكال والرسوم التوضيحية

الملخص التنفيذي

الهيئـة الوطنية للأمن السيبراني هي الجهة المختصّة بالأمن السيبراني في المملكة، والمرجع الوطني في شـؤونه؛ وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات والأنشطة الحكومية. وبناءً على تنظيم الهيئة الوطنية للأمن السيبراني، الصادر بالأمر الملكي الكريم ذي الرقم (٦٨٠١) والتاريخ ١٤٣٩/٢/١١هـ فإن اختصاصات الهيئة ومهماتها؛ تشمل وضع السياسات، والمعايير الوطنية للتشفير، ومتابعة الالتزام بها وتحديثها.

ومن هذا المنطلق؛ قامت الهيئة الوطنية للأمن السيبراني بمراجعة المعايير الوطنية للتشفير (NCS-1:2020) وتحديثها. وعلى هذا؛ فإن هذه النسخة (NCS-2:2025) ملغية للنسخة السابقة، وتحل ملحها.

تضع هذه الوثيقة (NCS-2:2025) الحد الأدنى لمتطلبات التشفير المقبولة للأغراض المدنية والتجارية، لحماية البيانات والأنظمة، والشبكات الوطنية. وتسلط هذه الوثيقة الضـوء على تفاصيل معايير التشفير الوطنية، التي تتكون من مستويين من القوة: أساسي ومتقدم.

تحدد الوثيقة الخوارزميات المتماثلة، وغير المتماثلة المقبولة، بما فيها خوارزميات التشفير، لما بعد الحوسبة الكمية؛ ويشمل ذلك تصاميم التشفير المتماثلة وغير المتماثلة، وكذلك بعض بروتوكولات التشفير المقبولة، وبنى المفاتيح التحتية، وإدارة دورة حياة المفاتيح، وتوليد الأعداد العشوائية؛ والتوزيع الكمي لمفاتيح التشفير؛ بالإضافة إلى ملاحق تتناول تقنيات التشفير المعززة للخصوصية، وهجمات القنوات الجانبية، والتشفير المبني على الهوية والسمات.

المقدمة

١-١ النطاق

تحدد المعايير الوطنية للتشفير (NCS-2:2025) الحد الأدنى لمتطلبات التشفير المطلوب من الجهات الوطنية الالتزام بها عند استخدام التشفير؛ لحماية البيانات (عند تخزينها أو معالجتها أو نقلها)، وكذلك الأنظمة والشبكات للأغراض المدنية والتجارية.

تم الأخذ في الحسبان عند إعداد وثيقة المعايير الوطنية للتشفير؛ الوضع الراهن، والتقدم المتوقع في القدرات الحوسبية. تشمل هذه الوثيقة أساسيات التشفير، وتصاميم التشفير، وبروتوكولات التشفير الشائعة، والبنية التحتية للمفاتيح العامة، وإدارة دورة المفاتيح، ومولدات الأعداد العشوائية، والتوزيع الكمي للمفاتيح.

يجب أن يتأكد الملتزمون بهذه المعايير، التطبيق الصحيح والآمن لها؛ لتفادي الثغرات الناتجة عن أخطاء التطبيق

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 جرى تصميم مستويات القوة؛ لتستهدف مستوى أمان 128-بت بالنسبة للمستوى الأساسي، ومستوى أمان 256-بت بالنسبة للمستوى المتقدم. وعلى كل جهة اختيار وتطبيق مستوى التشفير المناسب؛ حسب طبيعة البيانات والأنظمة والشبكات المراد حمايتها ومستوى حساسيتها. 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. إذا كان مستوى الأمان المستهدف هو المستوى المتقدم؛ فيجب أن تحقق كل نظم التشفير هذا المستوى وإذا كان مستوى الأمان المستهدف هو المستوى الأساسي، فيجب أن تحقق كل نظم التشفير إما المستوى الأساسي أو المتقدم. وقد جرى تحديد متطلبات محددة لكل مستوى في هذه الوثيقة. وعند الإشارة إلى متطلب غير مرتبط بمستوى قوة محدد؛ فسوف ينطبق المتطلب على كلا المستويين معا. يجري تحديد مستوى الأمان لنظم التشفير، حسب أقل مستوى أمان، لأي من مكونات نظام التشفير.

١-٣ هيكلية الوثيقة

جرى تنظيم بقية هذه الوثيقة على النحو الآتي: يعرض القسم الثاني من هذه الوثيقة، الخوارزميات المتماثلة، وغير المتماثلة المقبولة، شاملة أطوال المفاتيح، والكتل، ومتجهات التهيئة، وخوارزميات التشفير لما بعد الحوسبة الكمية. ويقدم القسم الثالث التصاميم المتماثلة وغير المتماثلة، وتشمل: طرق عمليات التشفير، ورموز توثيق الرسائل، والتشفير والتوثيق باستخدام البيانات المرتبطة، ودوال حماية المفاتيح، ودوال اشتقاق المفاتيح، والاتفاق على المفاتيح ونقلها، وتصاميم التشفير المتكامل، والتوقيع الرقمي، وتصاميم تشفير كامل المسار. كما يحتوي القسم الرابع على متطلبات التشفير لبروتوكولات التطبيقات الأكثر شيوعا وهي: بروتوكول الإنترنت الآمن (IPsec) وبروتوكول طبقة النقل الآمنة (TLS) وبرتوكول نظام اسم النطاق الآمن (DNSSEC) وبروتوكول الاتصال الآمن عن بعد (SSH) وبلوتوث (Bluetooth) ونظام الاتصالات المتنقلة العالمية (UMTS) والجيل الرابع (LTE) والجيل الخامس (5G) والوصول الآمن للشبكة اللاسلكية (WPA) وبروتوكول كيربيروس (KERBEROS). يعرض القسم ٥الخامس قائمة الخوارزميات، والمتطلبات للشهادات، وصلاحيتها. ويشمل القسم السادس متطلبات حماية المفاتيح وصلاحيتها، وكذلك عمليات إدارة دورة حياة المفاتيح؛ وذلك لضمان إدارة المفاتيح بشكل آمن من إنشائها حتى إتلافها. ولضمان الاستخدامات المعيارية لها خلال العمليات والإجراءات اللازمة. يقدم القسم السابع الحد الأدنى من المتطلبات الواجب تحقيقها عند استخدام مولدات الأعداد العشوائية. ويقدم القسم الثامن متطلبات التوزيع الكمي لمفاتيح التشفير. وأخيرا يقدم القسم التاسع ملاحق تتضمن بعض المعلومات عن التشفير، وتشمل تعزيز للخصوصية باستخدام التشفير، وهجمات القنوات الجانبية، والتشفير المبني على الهوية والسمات، والتعريفات والاختصارات، وجدول يبين التعديلات التي جرت على هذه الوثيقة. الشكل ١ يبين المكونات الأساسية والفرعية، للمعايير الوطنية للتشفير.

٢- أساسيات التشفير Cryptographic Primitives	٢-١	خوارزميات التشفير الانسيابية Stream Cipher Algorithms	٢-٢	خوارزميات التشفير الكتلية Block Cipher Algorithms
	٢-٣	دوال الاختزال Hash Functions	٢-٤	الخوارزميات غير المتماثلة الكلاسيكية Classical Asymmetric Algorithms
	٢-٥	خوارزميات ما بعد الحوسبة الكمية Post-Quantum Algorithms	٢-٦	خوارزميات التشفير الخفيفة Lightweight crypto Algorithms
٣- تصاميم التشفير Cryptographic Schemes	٣-١	طرق عمليات التشفير الكتلية Block Cipher Modes Of Operation	٣-٢	التشفير والتوثيق بالبيانات المرتبطة Authenticated Encryption With Associated Data (AEAD)
	٣-٣	رموز توثيق الرسائل Message Authentication Codes (MACS)	٣-٤	دوال حماية المفاتيح Key Wrap Functions
	٣-٥	دوال اشتقاق المفاتيح Key Derivation Functions (KDFs)	٣-٦	الاتفاق على المفاتيح ونقلها Key Agreement and Key Transport
	٣-٧	تصاميم التشفير المتكاملة Integrated Encryption Scheme	٣-٨	التوقيع الرقمي Digital Signatures
	٣-٩	تصاميم تشفير كامل المسار End-to-End Encryption (E2EE) Schemes		
٤- بروتوكولات التشفير الشائعة Commonly Used Protocols	٤-١	بروتوكولات الإنترنت الآمن IP Security (IPsec)	٤-٢	بروتوكول طبقة النقل الآمنة Transport Layer Security (TLS)
	٤-٣	بروتوكول نظام اسم النطاق الآمن Domain Name System Security (DNSSEC)	٤-٤	بروتوكول الاتصال الآمن عن بعد Secure Shell (SSH) Bluetooth
	٤-٥	بلوتوث Bluetooth	٤-٦	نظام الاتصالات المتنقلة العالمية (UMTS) / الجيل الرابع (LTE) / الجيل الخامس (5G)
	٤-٧	الوصول الآمن للشبكة اللاسلكية WPA (Wi-Fi Protected Access)	٤-٨	بروتوكول كيربيروس KERBEROS Protocol
٥- البنية التحتية للمفاتيح العامة Public Key Infrastructure (PKI)	٥-١	خوارزميات الشهادات Algorithms For Certificates	٥-٢	صلاحية الشهادات Validity Of The Certificates
٦- إدارة دورة المفاتيح Key Lifecycle Management	٦-١	حماية المفاتيح وصلاحيتها Key Protection and Lifetime	٦-٢	عمليات إدارة دورة حياة المفاتيح KLM Processes
٧- مولدات الأعداد العشوائية Random Number Generators (RNGs)	٧-١	مولدات الأعداد العشوائية المقبولة Acceptable Random Number Generators (RNGs)	٧-٢	المولدات للأعداد شبه العشوائية (PRNGS)
	٧-٣	بذرة العشوائية Random Seed	٧-٤	تجديد بذرة العشوائية Reseeding
	٧-٥	الاختبارات الإحصائية لمولدات الأعداد العشوائية RNGs Statistical Testing		
٨- التوزيع الكمى للمفاتيح Quantum Key Distribution (QKD)	٨-١	تنفيذ التوزيع الكمي للمفاتيح QKD Implementation	٨-٢	معدل خطأ البت الكمي Quantum Bit-Error Rate
	٨-٣	حماية حلول التوزيع الكمي للمفاتيح QKD protection	٨-٤	القيود الفنية Technical limitations
	٨-٥	الالتزام بمعايير التوزيع الكمي للمفاتيح QKD Standards		

شكل ٢: المكونات الرئيسية والفرعية للمعايير الوطنية للتشفير

أساسيات التشفير Cryptographic Primitives.

٢-١ خوارزميات التشفير الانسيابية Stream Cipher Algorithms

الخوارزميات المقبولة:

٢-١-١ SNOW 2.0 كما في ISO/IEC 18033-4

٢-١-١-١ طول المفتاح 128-بت للمستوى الأساسي.

٢-١-١-٢ طول المفتاح 256-بت للمستوى المتقدم.

٢-١-٢ SOSEMANUK[1] كما في eSTREAM project

٢-١-٢-١ طول المفتاح 128-بت و256-بت للمستوى الأساسي.

٢-١-٢-٢ غير مقبول للمستوى المتقدم.

٢-١-٣ يجب تحقيق المتطلبات الآتية عند استخدام خوارزميات التشفير الانسيابية:

٢-١-٣-١ يجب أن يكون طول متجه التهيئة Initialization Vector (IV) على الأقل 128-بت

٢-١-٣-٢ ألا يتكرر استخدام متجه التهيئة/الرقم الابتدائي (IV/nonce) خلال فترة استخدام المفتاح الواحد.

٢-١-٣-٣ لا يزيد استخدام المفتاح الواحد لتشفير أكثر من 2^{64}-بت.

٢-١-٣-٤ فك التشفير بصورة صحيحة لا يعد وسيلة مقبولة للتحقق من الموثوقية.

٢-٢ خوارزميات التشفير الكتلية Block Cipher Algorithms

الخوارزميات المقبولة هي:

٢-٢-١ معيار التشفير المتقدم (Advanced Encryption Standard "AES") كما في FIPS-197

٢-٢-١-١ طول المفتاح 128-بت و 192-بت، للمستوى الأساسي.

٢-٢-١-٢ طول المفتاح 256-بت، للمستوى المتقدم.

٢-٢-٢ Camellia كما في ISO/IEC 18033-3

٢-٢-٢-١ طول المفتاح 128-بت و 192-بت، للمستوى الأساسي.

٢-٢-٢-٢ طول المفتاح 256-بت، للمستوى المتقدم.

٢-٢-٣ Serpent[2]

٢-٢-٣-١ طول المفتاح 128-بت و 192-بت، للمستوى الأساسي.

[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.

٢-٢-٣-٢ طول المفتاح 256-بت، للمستوى المتقدم.

٢-٣ دوال الاختزال Hash Functions

الاختزال المقبولة هي:

٢-٣-١ دالة الاختزال Secure Hash Algorithm-2 (SHA-2)[3].

٢-١-٣-١ SHA2-256 وSHA2-384 وSHA2-512/256 للمستوى الأساسي، مع الاخذ بالاعتبار خطر هجمات تمديد الطول (Length Extension Attacks).

٢-١-٣-٢ SHA2-512 للمستوى المتقدم[4]، مع الاخذ في الحسبان خطر هجمات تمديد الطول (Length Extension Attacks).

٢-٣-٢ دالة الاختزال Secure Hash Algorithm-3 (SHA-3)

٢-٢-٣-١ SHA3-256 و SHA3-384 و SHAKE128 للمستوى الأساسي.

٢-٢-٣-٢ SHA3-512 وSHAKE256 للمستوى المتقدم.

٢-٣-٣ يجب تحقيق المتطلبات التالية

٢-٣-٣-١ دوال الاختزال يجب أن تكون مقاومة للانعكاس Inversion Resistant ومقاومة للتعارض Collision Resistant ومقاومة لإيجاد أصل الصورة Pre-image Resistant.

٢-٣-٣-٢ بالنسبة للخوارزمية SHAKE128 يجب أن يكون حجم مخرجاتها (d) أكبر من أو يساوي 256 بت.

٢-٣-٣-٣ بالنسبة للخوارزمية SHAKE256 يجب أن يكون حجم مخرجاتها (d) أكبر من أو يساوي 512 بت.

٢-٤ الخوارزميات غير المتماثلة الكلاسيكية Classical Asymmetric Algorithms

الخوارزميات المقبولة:

٢-٤-١ RSA

٢-٤-١-١ يكون طول (n) 3072 بت على الأقل وتكون قيمة (e) أكبر من أو يساوي 65537 للمستوى الأساسي.

٢-٤-١-٢ غير مقبول للمستوى المتقدم.

٢-٤-١-٣ يجب استخدام أعداد أولية قوية Strong Primes، كما جرى تعريفه في الملحق (هـ).

[3] SHA2-256 و SHA2-384 و SHA2-512/256 و SHA2-512 تكتب أحيانًا SHA2-256 وSHA2-384 وSHA2-512/256 وSHA2-512 على التوالي.

[4] تستخدم دالة الاختزال (SHA-384) عند تعذر تطبيق أحد الدوال المقبولة للمستوى المتقدم، مع الأخذ في الحسبان المخاطر السيبرانية وآلية التعامل معها.

٢-٤-٢ Diffie-Hellman

٢-٤-٢-١ يكون طول (p) 3072 بت على الأقل وتكون درجة العشوائية (entropy) للمفتاح الخاص 256 بت، للمستوى الأساسي.

٢-٤-٢-٢ غير مقبول، للمستوى المتقدم.

٢-٤-٢-٣ يجب استخدام أعداد أولية آمنة Safe Primes، كما جرى تعريفه في الملحق (هـ).

٢-٤-٣ Elliptic Curves

٢-٤-٣-١ المنحنيات NIST P-256 وNIST P-384 وBrainpoolP256r1 وBrainpoolP384r1 و Curve25519 للمستوى الأساسي.

٢-٤-٣-٢ المنحنيات NIST P-521 وCurve448[5] وBrainpoolP512r1 للمستوى المتقدم.

٢-٥ خوارزميات ما بعد الحوسبة الكمية Post-Quantum Algorithms

الخوارزميات المقبولة، لما بعد الحوسبة الكمية:

٢-٥-١ ML-KEM كما في FIPS 203

٢-٥-١-١ ML-KEM-512 وML-KEM-768 للمستوى الأساسي.

٢-٥-١-٢ ML-KEM-1024 للمستوى المتقدم.

٢-٥-٢ Classic McEliece

٢-٥-٢-١ mceliece348864، mceliece460896 للمستوى الأساسي.

٢-٥-٢-٢ mceliece6688128، mceliece6960119 و mceliece8192128 للمستوى المتقدم.

٢-٥-٣ ML-DSA كما في FIPS 204

٢-٥-٣-١ ML-DSA-44 و ML-DSA-65 للمستوى الأساسي.

٢-٥-٣-٢ ML-DSA-87 للمستوى المتقدم.

٢-٥-٤ SLH-DSA كما في FIPS 205

٢-٥-٤-١ للمستوى الأساسي: SLH-DSA-SHA2-128s،
SLH-DSA-SHAKE[6]-128f،
SLH-DSA-SHA2-128s،
أو SLH-DSA-SHA2-128f.

٢-٥-٤-٢ للمستوى المتقدم: SLH-DSA-SHA2-256s
أو SLH-DSA-SHAKE-256f.

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

[6] يُقبل استخدام SHAKE128 أو SHAKE256 بحجم أقل مما هو محدد في القسم ٣،٢ كاستثناء لخوارزميات PQC فحسب، وكما هو موصوف في FIPS 203، FIPS 204 و FIPS 205.

٢-٥-٤-٣ لا يزيد استخدام المفتاح الواحد لتوقيع أكثر من 2^{64} رسالة.

٢-٥-٥ على نظم التشفير لما بعد الحوسبة الكمية تحقيق المتطلبات الآتية:

٢-٥-٥-١ يجب استخدام نظم التشفير لما بعد الحوسبة الكمية؛ مع نظم تشفير كلاسيكية.

٢-٥-٥-٢ يجب أن تدعم جميع نظم وحلول التشفير خوارزميات التشفير لما بعد الحوسبة الكمية (PQC).

٢-٦ خوارزميات التشفير الخفيفة Lightweight crypto Algorithms

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

٢-٦-١ خوارزميات التشفير الكتلية Block Ciphers كما في ISO/IEC 29192-2

٢-١-٦-١ PRESENT طول المفتاح 80-بت أو 128-بت.

٢-١-٦-٢ CLEFIA طول المفتاح 128-بت أو 192-بت أو 256-بت.

٢-٦-٢ خوارزميات التشفير الانسيابية Stream Ciphers كما في ISO/IEC 29192-3

٢-٢-٦-١ Enocoro طول المفتاح 80-بت أو 128-بت.

٢-٢-٦-٢ Trivium طول المفتاح 80-بت.

٢-٦-٣ الخوارزميات الغير متماثلة Asymmetric Algorithms كما في ISO 29192-4

٢-٣-٦-١ Unilateral

٢-٣-٦-٢ ALIKE

٢-٣-٦-٣ Identity-based signatures

٢-٦-٤ دوال الاختزال Hash Functions كما في ISO 29192-5

٦-٤-٢-١ PHOTON حجم المخرجات 80-بت أو 128-بت أو 160-بت أو 224-بت أو 256-بت.

٦-٤-٢-٢ SPONGNET حجم المخرجات 88-بت أو 128-بت أو 160-بت أو 224-بت أو 256-بت.

٦-٤-٢-٣ Lesamnta-LW حجم المخرجات 256-بت.

٢-٦-٥ رموز توثيق الرسائل Message Authentication Code (MAC) كما في ISO 29192-6

١،٥،٦،٢ Tsudik's keymode, hash based

٢،٥،٦،٢ Chaskey12، طول المفتاح 128-بت.

٢-٦-٦ التشفير والتوثيق باستخدام البيانات المرتبطة Authenticated encryption with associated data (AEAD) كما في NIST SP 800-232

٢-٦-٦-١ Ascon، طول المفتاح 128-بت أو 160-بت.

تصاميم التشفير Cryptographic Schemes

يستعرض هذا القسم تصاميم التشفير المقبولة؛ التي يجري استخدامها، مع أساسيات التشفير الواردة في القسم ٣ أو أي أساسيات أخرى، بمستوى الأمان نفسه أو أعلى.

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

طرق عمليات التشفير الكتلية المقبولة هي:

٣-١-١ طريقة التشفير باستخدام العداد (Counter Mode "CTR")، كما في NIST SP800-38A و RFC 3686.

٣-١-٢ Cipher Block Chaining (CBC) كما في NIST SP800-38A للمستوى الأساسي فحسب.

٣-١-٣ طريقة التشفير باستخدام المخرجات للتغذية الراجعة (Output Feedback "OFB")، كما في NIST SP 800-38A.

٣-١-٤ طريقة التشفير بالتغذية الراجعة (Cipher Feedback "CFB")، كما في NIST SP 800-38A.

٣-١-٥ لجميع طرق عمليات التشفير الآنفة الذكر، يجب ألا يزيد استخدام المفتاح، لأكثر من 2^{32} من كتل البيانات (blocks of data)، وأن يكون متجه التهيئة/القيمة الابتدائية عشوائي عند كل تشفير باستخدام المفتاح الواحد.

٣-١-٦ طريقة التشفير الخاصة بأنظمة التخزين (XEX Tweakable Block Cipher with Ciphertext Stealing "XTS")، كما في NIST SP800-38E، بحيث لا يزيد حجم وحدات البيانات المشفرة باستخدام المفتاح الواحد عن 2^{20} كتلة.

٣-٢ التشفير والتوثيق باستخدام البيانات المرتبطة Authenticated Encryption with Associated Data (AEAD)

التصاميم المقبولة للتشفير والتوثيق؛ باستخدام البيانات المرتبطة، هي:

٣-٢-١ طريقة التشفير والتوثيق؛ باستخدام عداد جالوا (Galois Counter Mode "GCM") كما في NIST SP 800-38D مع تحقيق الآتي:

٣-١-٢-١ طول متجه التهيئة/الرقم الابتدائي (IV/nonce) على الأقل 128-بت.

٣-١-٢-٢ ألا يتكرر استخدام متجه التهيئة/الرقم الابتدائي (IV/nonce) خلال فترة استخدام المفتاح الواحد.

٣-١-٢-٣ أن يكون طول الوسم (tag) 128-بت، على الأقل.

٣-١-٢-٤ لا يزيد استخدام المفتاح الواحد عن أكثر من 2^{64} من كتل البيانات (blocks of data).

٣-٢-٢ طريقة التشفير والتوثيق، باستخدام العداد، مع تسلسل كتل التشفير (Counter with CBC MAC "CCM") كما في NIST SP 800-38C مع تحقيق الآتي:

٣-٢-٢-١ ألا يتكرر استخدام متجه التهيئة/الرقم الابتدائي (IV/nonce) خلال فترة استخدام المفتاح الواحد.

٣-٢-٢-٢ أن يكون طول الوسم (tag) 128-بت على الأقل.

٣-٢-٢-٣ لا يزيد استخدام المفتاح الواحد لأكثر من 2^{61} استدعاء[7] لخوارزمية التشفير الكتلية.

٣-٣ رموز توثيق الرسائل Message Authentication Codes (MACs)

تصاميم رموز توثيق الرسائل المقبولة (مع الاخذ بالاعتبار بأن طول المفتاح يجب أن يتماشى على الأقل مع مستوى الأمان المستهدف) هي:

٣-٣-١ رموز توثيق الرسائل باستخدام دوال الاختزال (Hash-based MAC "HMAC") كما في FIPS PUB 198-1 مع تحقيق الآتي:

٣-٣-١-١ يجب أن يتسق طول الوسم (tag) وطول المفتاح على الأقل؛ مع مستوى الأمان المستهدف (للمستوى الأساسي والمتقدم).

٣-٣-١-٢ يستخدم مع دوال تجزئة (Hash functions) مقبولة؛ كما هو مذكور في القسم ٣،٢.

٣-٣-٢ رموز توثيق الرسائل بالتشفير (Cipher-based MAC "CMAC") كما في NIST SP 800-38B مع تحقيق الآتي:

٣-٣-٢-١ المفتاح يجب أن يتسق على الأقل مع مستوى الأمان المستهدف (للمستوى الأساسي والمتقدم).

٣-٣-٢-٢ لا يزيد استخدام المفتاح الواحد إلى أكثر من 2^{48} من كتل الرسالة (message blocks).

٣-٣-٢-٣ يقتصر استخدامها على التطبيقات التي لا يستطيع أي طرف معرفة تشفير سلسة الأصفار (all-0 Strings).

٣-٣-٢-٤ أن يكون طول الوسم (tag) على الأقل 128-بت

٣-٣-٣ رموز توثيق الرسائل (KECCAK Message Authentication Code "KMAC") كما في NIST SP 800-185.

٣-٣-٣-١ يجب أن يتماشى طول الوسم (tag) وطول المفتاح على الأقل مع مستوى الأمان المستهدف (للمستوى الأساسي والمتقدم).

٣-٣-٣-٢ تستخدم مع خوارزميات اختزال آمنه، ومعدلة باستخدام كاتشاك KECCAK (cSHAKE128 و cSHAKE256) بما يتناسب مع مستوى الأمان المستهدف (المستوى الأساسي أو المستوى المتقدم)

٣-٣-٤ رموز توثيق الرسائل GMAC كما في NIST SP 800-38D.

٣-٣-٤-١ المفتاح يجب أن يتسق على الأقل؛ مع مستوى الأمان المستهدف (للمستوى الأساسي والمتقدم).

٣-٣-٤-٢ طول متجه التهيئة/الرقم الابتدائي (IV/nonce) على الأقل 128-بت.

٣-٣-٤-٣ أن يكون طول الوسم (tag) على الأقل 128-بت.

٣-٣-٤-٤ لا يزيد استخدام المفتاح الواحد عن أكثر من 2^{64} من كتل البيانات (blocks of data).

[7] أي عدد مرات تنفيذ خوارزمية التشفير الكتلية (مثل AES) باستخدام مفتاح واحد .

٣-٤ دوال حماية المفاتيح Key Wrap Functions

تصاميم حماية المفاتيح المقبولة هي:

٣-٤-١ تغليف المفاتيح وحمايتها (Key Wrap "KW") كما في NIST SP 800-38F .

٣-٤-٢ تغليف المفاتيح وحمايتها مع التعبئة (Key Wrap with Padding "KWP") كما في NIST SP 800 38F.

٣-٥ دوال اشتقاق المفاتيح Key Derivation Functions (KDFs)

تصاميم دوال اشتقاق المفاتيح المقبولة هي:

٣-٥-١ RFC 5869 (HKDF)[8].

٣-٥-٢ IKE-v2-KDF[8].

٣-٥-٣ TLS-v1.2-KDF[8].

٣-٥-٤ X9.63-KDF[8].

ويجب أن تكون متوافقة مع التالي:

٣-٥-٥ NIST SP-800-56 A/B KDF (Single Step)[8].

٣-٥-٦ SP-800-56 C KDF (Extract-then-expand)[8].

٣-٥-٧ NIST SP-800-108[8].

٣-٥-٨ NIST SP-800-135.

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

التصاميم المقبولة لتبادل المفاتيح:

٣-٦-١ RSA Key Establishment كما في NIST 800-56B.

٣-٦-١-١ طول المفتاح 3072 بت على الأقل للمستوى الأساسي.

٣-٦-١-٢ غير مقبول للمستوى المتقدم.

٣-٦-٢ Diffie-Helman (DH) كما في RFC 3526.

٣-٦-٢-١ طول المفتاح 3072 بت على الأقل للمستوى الأساسي.

٣-٦-٢-٢ غير مقبول للمستوى المتقدم.

٣-٦-٣ Elliptic Curve Diffie-Hellman (ECDH) كما في NIST SP 800-56A.

٣-٦-٣-١ يجب استخدام المنحنيات المقبولة في ٣،٤،٢.

٣-٦-٣-٢ مع تمكين خاصية Forward Secrecy وتطبيق إنشاء المفاتيح الموثقة.

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

٣-٦-٤ تصاميم تبادل المفاتيح المتماثلة:

٣-٦-٤-١ تتحقق التصاميم المقبولة؛ للاتفاق على المفاتيح، باستخدام بيانات سرية مشتركة، طويلة المدى فحسب.

٣-٦-٤-٢ يمكن استخدام كل تصاميم التشفير وأساسياته المتماثلة، المذكورة في القسم ٣ والقسم ٤.

٣-٦-٤-٣ تتحقق التصاميم المقبولة لنقل المفاتيح، بالجمع بين تصاميم التشفير، والتوثيق باستخدام رموز توثيق الرسائل (MAC) بطريقة التشفير، ثم التوثيق (encrypt-then-MAC).

٣-٦-٤-٤ يجب حماية كل المفاتيح بدوال حماية المفاتيح (Key Wrap Functions) المذكورة في القسم ٣،٤.

٣-٧ تصاميم التشفير المتكاملة Integrated Encryption Scheme

التصاميم المقبولة:

٣-٧-١ Elliptic Curve Integrated Encryption Scheme (ECIES) للمستوى الأساسي والمستوى المتقدم.

٣-٧-٢ Discrete Logarithm Integrated Encryption Scheme (DLIES) للمستوى الأساسي فحسب.

٣-٧-٣ RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP) كما في PKCS#1 v2.1:RSA للمستوى الأساسي فحسب.

٣-٨ التوقيع الرقمي Digital Signatures

التواقيع الرقمية المقبولة هي:

٣-٨-١ Digital Signature Algorithm (DSA) كما في FIPS PUB 186-4.

٣-٨-١-١ طول المفتاح 3072-بت على الأقل للمستوى الأساسي.

٣-٨-١-٢ غير مقبول للمستوى المتقدم.

٣-٨-٢ Elliptic Curve Digital Signature Algorithm (ECDSA) و Edwards-curve Digital Signature Algorithm (EdDSA) كما في FIPS PUB 186-5.

٣-٨-٢-١ يجب استخدام المنحنيات المقبولة في ٣،٤،٢.

٣-٨-٣ RSA signatures.

٣-٨-٣-١ التصاميم المقبولة RSA-PSS و RSA Digital Signature Scheme (RSA-DS2)[9,10] .

٣-٨-٣-٢ طول المقياس (Modulus) 3072-بت على الأقل للمستوى الأساسي.

٣-٨-٣-٣ غير مقبول للمستوى المتقدم.

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

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

٣-٨-٤ Merkle.

٣-٨-٤-١ يجب استخدام دوال الاختزال Hash Functions المقبولة في القسم ٢.

٣-٨-٤-٢ يجب أن يكون مولد الأعداد شبه العشوائية Pseudo-Random مبني باستخدام HMAC بناءً على دوال الاختزال المستخدمة.

٣-٩ تصاميم تشفير كامل المسار End-to-End Encryption (E2EE) Schemes

٣-٩-١ يجب اقتصار تصاميم تشفير كامل المسار (E2EE) بشأن عملية التشفير (Encryption) وفك التشفير (Decryption) على النهايات الطرفية المصرح لها بذلك.

٣-٩-٢ يجب أن تكون البيانات غير المشفرة (Plaintext) والمعلومات الخاصة بالمفاتيح (Keying Materials) غير متاحة لأي نظام أو جهة وسيطة (مثل الخوادم أو أجهزة البنية التحتية للشبكة، أو مزودي الخدمات).

٣-٩-٣ يجب على تصاميم تشفير كامل المسار (E2EE) توفير خاصية (Forward Secrecy) عن طريق تبادل المفاتيح المؤقتة (Ephemeral Key Exchange).

٣-٩-٤ يجب أن توفّر تصاميم تشفير كامل المسار (E2EE) وسيلة تتيح للنهايات الطرفية التحقق من هويات المستخدمين، سواء من خلال استخدام الشهادات الرقمية، أو المفاتيح العامة المُوثقة (Authenticated Public Keys)، أو المفاتيح السرية التي جرى المشاركة بها مسبقاً (Pre- shared Secrets).

٣-٩-٥ يجب أن توفّر تصاميم تشفير كامل المسار (E2EE) للمستخدمين إمكانية التحقق المستقل من مفاتيح التشفير السرية المؤقتة (Session Keys)، على سبيل المثال، من خلال التحقق خارج النطاق (out- of- band).

بروتوكولات التشفير الشائعة

Commonly Used Cryptographic Protocols

يستعرض هذا القسم المتطلبات الفنية المقبولة، من بروتوكولات التشفير الشائعة الاستخدام. يجب الأخذ في الحسبان 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 الآتية المدرجة، يجب أن تطبق عليها أيضا، المتطلبات المذكورة في القسم ٢ والقسم ٣.

٤-١ بروتوكولات الإنترنت الآمن IP Security (IPsec)

المتطلبات المقبولة:

لاستخدامات التوثيق Authentication فحسب؛ يمكن استخدام أحد الخوارزميات الآتية[11]:

٤-١-١ للمستوى الأساسي:

.ENCR_NULL_AUTH_AES_GMAC_128

.AUTH_HMAC_SHA2_256 _128

.AUTH_HMAC_SHA2_384_192

.AUTH_HMAC_SHA3_256_128

.AUTH_HMAC_SHA3_384_192

٤-١-٢ للمستوى المتقدم:

.ENCR_NULL_AUTH_AES_GMAC_256

.AUTH_HMAC_SHA2_512_256

.AUTH_HMAC_SHA3_512_256

للاستخدامات المتطلبة للسرية Confidentiality مع التوثيق Authentication. يجب استخدام تغليف البيانات الآمن Encapsulating Security Payload (ESP) عن طريق استخدام أحد تصاميم التوثيق MAC الآنفة، مع أحد خوارزميات التشفير الآتية[12]:

٤-١-٣ .ENCR_AES_CTR

.ENCR_CAMELLIA_CTR

و يمكن استخدام التشفير والتوثيق باستخدام إحدى الطرق الآتية بوصفها خياراً آخر:

٤-١-٤ ENCR_AES_CCM_12،

ENCR_AES_CCM_16،

ENCR_CAMELLIA_CCM_12،

ENCR_CAMELLIA_CCM_16،

[11] يوصى بعدم استعمال أو تطبيق حقل التوثيق Authentication Header (AH).

[12] European Union Agency for Network and Information Security “Study on cryptographic protocols,” 2014.

،ENCR_AES_GCM_12
.ENCR_AES_GCM_16

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

الإصدارات المقبولة:

٤-٢-١ يقبل استخدام TLS 1.2 مع أساسيات التشفير المقبولة وتصاميمه، حسب المتطلبات في القسم ٢ والقسم ٣ لضمان التوافق، وتطبيق إعدادات لا تسمح بخفض مستوى الأمان[13].

٤-٢-٢ ينصح باستخدام المعيار TLS 1.3.

المتطلبات المقبولة في TLS 1.2

٤-٢-٣ الخوارزميات التالية مقبولة للمستوى الأساسي:

،TLS_ ECDHE_ECDSA_WITH_AES_128_CBC[14] _ SHA2_256

،TLS_ ECDHE_ECDSA_WITH_AES_256_CBC[14]_SHA2_384

،TLS_ ECDHE_ECDSA_WITH_AES_128_GCM_SHA2_256

،TLS_ ECDHE_ECDSA_WITH_AES_128_CCM

،TLS_ ECDHE_ECDSA_WITH_AES_128_CCM_8

،TLS_ ECDHE_RSA_WITH_AES_128_ CBC[14]_SHA2_256

،TLS_ ECDHE_RSA_WITH_AES_256_ CBC[14]_SHA2_384

،TLS_ ECDHE_RSA_WITH_AES_128_GCM_ SHA2_256

.TLS_ ECDHE_RSA_WITH_AES_256_GCM_SHA2_384

٤-٢-٤ الخوارزميات التالية مقبولة للمستوى المتقدم:

،TLS_ ECDHE_ECDSA_WITH_AES_256_GCM_SHA2_384

،TLS_ECDHE_ ECDSA _WITH_AES_256_CCM

.TLS_ECDHE_ ECDSA _WITH_AES_256_CCM_8

المتطلبات المقبولة في TLS 1.3

٤-٢-٥ TLS_AES_128_GCM_SHA256 للمستوى الأساسي.

٤-٢-٦ TLS_AES_256_GCM_SHA384 للمستوى المتقدم.

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

المتطلبات المقبولة لتوقيع بيانات المنطقة Zone Data Signing:

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

[14] يجب استعمال CBC مع امتداد التشفير مع التوثيق (Encrypt_then_MAC).

٤-٣-١ ECDSA_P256_SHA256 و ED25519 للمستوى الأساسي.

٤-٣-٢ ECDSA_P384_SHA384[15] و ED488 للمستوى المتقدم.

المتطلبات لتوثيق الرسائل Message Authentication:

٤-٣-٣ HMAC_SHA384 للمستوى الأساسي.

٤-٣-٤ HMAC_SHA512 للمستوى المتقدم.

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

الإصدار المقبول لبروتوكول الاتصال الآمن عن بعد، هو SSH-2 مع خوارزميات التشفير والتوثيق الآتية:

٤-٤-١ AEAD_AES_128_GCM للمستوى الأساسي.

٤-٤-٢ AEAD_AES_256_GCM للمستوى المتقدم.

٤-٥ بلوتوث Bluetooth

الإصدارات المقبولة:Bluetooth 4.1 أو أعلى كما في NIST SP 800-121r2 مع المتطلبات الآتية:

٤-٥-١ استخدام وضع الأمان ٤ (Security Mode 4)، المستوى ٤ (Level 4) مع مفتاح اتصال موثق، وباستخدام قنوات آمنة.

٤-٥-٢ استخدام خوارزمية التشفير AES-CCM.

٤-٥-٣ استخدام خاصية الاتصال الآمن، مع ECC P-256 لإنشاء مفتاح الاتصال.

٤-٥-٤ استخدم وضع أمان التشفير ٣ (Encryption Mode 3) مع تشفير جميع المراسلات (Encrypt All Traffic).

٤-٥-٥ 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).

٤-٥-٦ يجب استخدام أقوى أوضاع الأمان المتاحة، في أجهزة البلوتوث.

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

المتطلبات المقبولة:

٤-٦-١ بالنسبة لنظام الاتصالات المتنقلة العالمية (UMTS) يجب استخدام 128-UEA1 مع 128-UIA1.

٤-٦-٢ بالنسبة للجيل الرابع (LTE) يجب استخدام 128-EEA2 مع 128-EIA2.

٤-٦-٣ بالنسبة للجيل الخامس (5G) يجب استخدام 128-NEA2 مع 128-NIA2 أو 256-NEA2 مع 256-NIA5

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

٤-٦-٤ يمكن استخدام EIA0 و NIA0 في الحالات الاستثنائية للمكالمات الطارئة، غير الموثقة Unauthenticated في وضع الخدمة المحدودة Limited Service Mode.

٤-٦-٥ يجب استخدام أساسيات وتصاميم التشفير، المذكورة في القسم ٢ والقسم ٣ فحسب. ويمكن استخدام خوارزمية KASUMI و ECIES Profile A و ECIES Profile B بوصفها استثناء خاص ومقبول لأنظمة 3GPP.

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

الإصدارات المقبولة:

٤-٧-١ WPA3-Enterprise

٤-٨ بروتوكول كيربيروس Kerberos Protocol

المتطلبات المقبولة:

٤-٨-١ للمستوى الأساسي: CAMELLIA128-CTS-CMAC،
AES256-CTS-HMAC-SHA384.

٤-٨-٢ للمستوى المتقدم: CAMELLIA256-CTS-CMAC.

البنية التحتية للمفاتيح العامة

Public Key Infrastructure (PKI)

٥-١ خوارزميات الشهادات Algorithms for Certificates

الخوارزميات المقبولة لشهادات الجذرية Root CA Certificates:

٥-١-١ RSA.

٥-١-١-١ طول المفتاح 4096-بت على الأقل.

٥-١-٢ ECC.

٥-١-٢-١ 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:

٥-١-٣ RSA.

٥-١-٣-١ طول المفتاح 3072-بت على الأقل.

٥-١-٤ ECC.

٥-١-٤-١ NIST P-384 و NIST P-521 و Curve448 و BrainpoolP384r1 و BrainpoolP512r1.

يجب تحقيق المتطلبات التالية:

٥-١-٥ أن تتوافق الشهادات (Certificates) وقائمة الشهادات الملغية (Certificate Revocation Lists "CRLs") وقائمة الهيآت الملغية (Authority Revocation Lists "ARLs") مع X.509 PKI Certificate كما في RFC 5280.

٥-١-٦ يجب استخدام دوال اختزال Hash function المقبولة في القسم ٢.

٥-١-٧ يجب أن يتوافق مستوى قوة خوارزميات المفاتيح غير المتماثلة Asymmetric Key Algorithms مع مستوى قوة خوارزميات الاختزال Hash Algorithms.

٥-٢ صلاحية الشهادات Validity of the Certificates

فترة صلاحية الشهادات الجذرية Root CA Certificates:

٥-٢-١ ٢٠ سنة في الحد الأقصى.

فترة صلاحية شهادات هيآت الشهادات المتوسطة والثانوية المانحة Intermediate CA, Subordinate CA and Issuing CA:

٥-٢-٢ ١٠ سنوات في الحد الأقصى.

فترة صلاحية شهادات المستخدم النهائي End User Certificate:

٥-٢-٣ ٥ سنوات في الحد الأقصى للمستوى الأساسي[16].

٥-٢-٤ ٣ سنوات في الحد الأقصى للمستوى المتقدم[16].

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

إدارة دورة المفاتيح

Key Lifecycle Management

٦-١ حماية المفاتيح وصلاحيتها Key Protection and Lifetime

حماية المفاتيح وصلاحيتها المقبولة:

٦-١-١ استخدام أجهزة وحدات التشفير Hardware Cryptographic Modules

٦-١-١-١ يجب أن تكون المفاتيح الخاصة Private Keys صالحة لمدة لا تزيد عن ٥ سنوات (لا يحد هذا من فترة صلاحية شهادات هيئات الشهادات CA Certificates) للمستوى الأساسي[17].

٦-١-١-٢ يجب أن تكون المفاتيح الخاصة Private Keys صالحة لمدة لا تزيد عن ٣ سنوات (لا يحد هذا من فترة صلاحية شهادات هيئات الشهادات CA Certificates) للمستوى المتقدم[17].

٦-١-٢ استخدام برمجيات وحدات التشفير Software Cryptographic Modules.

٦-١-٢-١ لا يسمح أن تكون المفاتيح Private Keys صالحة لأكثر من سنتين للمستوى الأساسي[17].

٦-١-٢-٢ غير مقبول للمستوى المتقدم.

٦-٢ عمليات إدارة دورة حياة المفاتيح KLM Processes

متطلبات إدارة دورة حياة المفاتيح التي يجب الالتزام بها هي:

٦-٢-١ إنشاء المفاتيح Key Generation

٦-٢-١-١ يجب إنشاء المفاتيح باستخدام مصدر عشوائي؛ غير قابل للتنبؤ أو الانحياز (كما في القسم ٧).

٦-٢-٢ تسجيل المفاتيح وتصديقها Key Registration and Certification

٦-٢-٢-١ يجب أن تكون المفاتيح العامة، مرتبطة بأصحابها من خلال الشهادات.

٦-٢-٢-٢ يجب توزيع الشهادات الجذرية (Root certificates) على الأطراف المعتمدة بطريقة آمنة.

٦-٢-٢-٣ يجب استخدام هيئات شهادات وطنية موثوقة، ومعتمدة من الجهة، أو صاحب الصلاحية.

٦-٢-٣ توزيع المفاتيح وتثبيتها Key Distribution and Installation

٦-٢-٣-١ يجب توزيع المفاتيح على مستخدميها بطريقة آمنة، وأن تكون تحت تحكم المستخدم.

٦-٢-٣-٢ يجب نقل المفاتيح بطريقة آمنة؛ مع التأكيد على حماية سريتها وموثوقيتها.

٦-٢-٣-٣ يجب تثبيت جميع نسخ المفاتيح، وتخزينها بأمان.

٦-٢-٣-٤ يجب نقل المفاتيح العامة، بطريقة موثوقة، باستخدام الشهادات.

٦-٢-٣-٥ يجب حماية المفاتيح الخاصة، وأن يكون استخدامها مصرح به من قبل المالك، أو هيئة الشهادات.

[17] NIST, "NIST Special Publication 800-57 Part 1 Revision 4. Recommendation for Key Management Part 1: General. Elaine Barker," 2016.

٦-٢-٣-٦ عند حماية مفاتيح التشفير أو نقلها أو مصادقتها؛ يجب استخدام آليات تشفير، توفر مستوى قوة يعادل قوة مفتاح التشفير المراد حمايته أو يفوقه، أو يعادل قوة مفاتيح مالك الشهادة.

٦-٢-٤ استخدام المفاتيح Key Use

٦-٢-٤-١ يجب حماية المفاتيح، ضد الاستخدام غير المصرح به، منذ إنشائها، وحتى إتلافها.

٦-٢-٤-٢ يجب حماية المفاتيح، ضد إساءة الاستخدام من مُلاكها، وذلك بتخزينها على جهاز آمن، والتأكد من منح الصلاحيات ومراقبتها.

٦-٢-٥ تخزين المفاتيح Key Storage

٦-٢-٥-١ يجب على الجهات، أن تحتفظ بنسخ احتياطية آمنة للمفاتيح (للاستخدام الداخلي أو عند تطبيق القانون) وذلك في حال كون خوارزميات التشفير، ماتزال مستخدمة.

٦-٢-٥-٢ يجب أن تكون المفاتيح المستخدمة لغرض التوثيق، وعدم الإنكار؛ تحت التحكم الحصري من قبل المستخدم.

٦-٢-٦ إلغاء المفاتيح والتحقق من صحتها Key Revocation and Validation

٦-٢-٦-١ يجب اعتماد إصدارات محدثة، لقائمة الشهادات الملغية (Certificate Revocation List "CRL")وبروتوكول حال الشهادة عبر الإنترنت (Online Certificate Status Protocol "OCSP") لتفادي استخدام مفاتيح منتهية الصلاحية، أو جرى إلغاؤها.

٦-٢-٦-٢ يجب التحقق من صحة المفاتيح؛ عن طريق التأكد من خوادم قائمة الشهادات الملغية "CRL" أو بروتوكول حال الشهادة عبر الإنترنت "OCSP".

٦-٢-٧ أرشفة المفاتيح Key Archival

٦-٢-٧-١ يجب أرشفة المفاتيح ذات الصلاحية المنتهية، أو الملغية؛ لضمان الوصول إلى البيانات القديمة، وذلك في حال كانت خوارزميات التشفير ماتزال مستخدمة.

٦-٢-٧-٢ يجب أن تكون عملية الأرشفة آمنة، إضافةً إلى ضمان سرية المفاتيح المُؤرشفة.

٦-٢-٧-٣ يجب أن تتبع أنظمة الأرشفة فترات الاحتفاظ المطلوبة، وفقاً للتنظيمات ذات العلاقة.

٦-٢-٨ إتلاف المفاتيح Key Destruction

٦-٢-٨-١ يجب حذف المفاتيح من جهاز التخزين بطريقة آمنة، عند انتهاء صلاحيتها، ولم يكن هناك حاجة لتخزينها أو أرشفتها.

٦-٢-٨-٢ عند حذف المفاتيح؛ يجب اتباع الإجراءات ذات العلاقة، بحسب ما يصدر من الهيئة الوطنية للأمن السيبراني، في هذا الشأن

٦-٢-٩ المحاسبة على المفاتيح Key Accounting

٦-٢-٩-١ يجب وضع آلية للمحاسبة، على المفاتيح غير المتماثلة، خلال دورة حياتها.

٦-٢-٩-٢ يجب مراقبة استخدام المفاتيح.

٦-٢-٩-٣ يجب أن تكون المهمات والمسؤوليات لإدارة المفاتيح، موثقة، وموافق عليها، من قبل صاحب الصلاحية.

٦-٢-١٠ استرداد /استعادة المفاتيح Key Recovery

٦-٢-١٠-١ يجب أن تكون إجراءات استعادة المفاتيح موثقة، وموافق عليها، من قبل صاحب الصلاحية.

مولدات الأعداد العشوائية

Random Number Generators (RNGs)

يجب تحقيق المتطلبات الآتية:

١-٧ أن يتم استخدام مولدات الأعداد ذات العشوائية التامة (True Random Number Generators "TRNGs")أو المولدات الكمية للأعداد العشوائية (Quantum Random Number Generators "QRNGs") أو المولدات الهجينة للأعداد شبه العشوائية (Hybrid Pseudo Random Number Generators "Hybrid-PRNGs") في أنظمة التشفير،

٢-٧ يمنع استخدام المولدات المحددة للأعداد شبه العشوائية (PRNGs) مع مصدر للعشوائية، محدد وقابل للتوقع (deterministic and predictable).

٣-٧ أن تكون بذرة العشوائية (seed) المستخدمة لتوليد الأعداد شبه العشوائية (PRNG) حديثة وبدرجة عشوائية تساوي ١٢٨-بت للمستوى الأساسي، و٢٥٦-بت للمستوى المتقدم، كما يجب إنشاؤها، من مصدر ذي درجة عشوائية عالية وموثوق، وغير محدد (non-deterministic entropy source).

٤-٧ أن يعاد تجديد البذرة العشوائية (reseeding) عند فترات محددة، أو عند طلب المكوّن الذي يستخدم الأعداد العشوائية؛ وذلك في مولدات الأعداد العشوائية (PRNGs).

٥-٧ أن تجتاز مولدات الأعداد العشوائية الاختبارات الإحصائية المعيارية، للأعداد العشوائية؛ قبل اعتمادها لأنظمة التشفير (offline testing) باستخدام مجموعات الاختبارات الإحصائية الحديثة؛ مثل مجموعات الاختبارات الصادرة من المعهد الوطني للمعايير والتقنية (NIST) كما في (NIST SP 800-22) و (Dieharder)[18].

[18] R. G. Brown "Dieharder: A Random Number Test Suite", Oct 2022. https://webhome.phy.duke.edu/~rgb/ General/dieharder.php

التوزيع الكمي للمفاتيح
Quantum Key Distribution (QKD)

يجب تحقيق المتطلبات الآتية عند استخدام أنظمة التوزيع الكمي للمفاتيح (QKD) وحلولها:

٨-١ يجب تنفيذ التوزيع الكمي للمفاتيح QKD بطريقة هجينة؛ تستخدم خوارزميات ما بعد الحوسبة الكمية (Post-Quantum) مع الخوارزميات الكلاسيكية، أو أحدهما؛ للتوثيق (Authentication) والاتفاق على المفاتيح (Key Agreement).

٨-٢ يجب مراقبة معدل خطأ البت الكمي (Quantum Bit Error Rate-QBER) بشكل مستمر؛ لاكتشاف أي تداخل (Interference).

٨-٣ تجب حماية حلول التوزيع الكمي للمفاتيح (QKD) من الهجوم الوسيط (Man-in-the-Middle) مثل هجمات الوسيط المادية؛ التي تستهدف البنية التحتية للشبكات.

٨-٤ الأخذ في الحسبان القيود الفنية، عند تطبيق أنظمة التوزيع الكمي لمفاتيح التشفير (QKD) وحلوله والمخاطر السيبرانية، المصاحبة لها، وآلية التعامل معها.

٨-٥ يجب على الجهة المستخدمة لحلول التوزيع الكمي لمفاتيح التشفير (QKD) أن تكون متوافقة على الأقل، مع أحد المعايير الآتية:

٨-٥-١ ISO/IEC 23837.

٨-٥-٢ ETSI GS QKD 008 و ETSI GS QKD 016.

الملاحق

الملحق (أ) التشفير المعزز للخصوصية Privacy-Enhancing Cryptography

تشمل التطورات الحديثة في التشفير المعزز للخصوصية (Privacy-Enhancing Cryptography, PEC) تقنيات تشفير متخصصة؛ تمكن من معالجة البيانات، أو تحليلها، دون كشف محتواها. فعلى سبيل المثال، تستخدم هذه الأساليب لإجراء الحسابات على البيانات الحساسة ومعالجتها على السحابة، بحيث تظل البيانات آمنة، حتى أثناء استخدامها بصورة نشطة. وفيما يلي أمثلة أساسية على هذه التصاميم:

١- التشفير المتشاكل Homomorphic Encryption (HE)

يُستخدم التشفير المتشاكل (HE) لإتاحة إجراء حسابات آمنة، على البيانات الخاصة؛ من خلال معالجة النصوص المشفرة فحسب. المعايير المتعلقة بالتشفير المتشاكل، وخاصة في ما يتعلق بالتشفير المتشاكل بالكامل (Fully-Homomorphic Encryption-FHE) -الذي يتيح إجراء أي عملية حسابية على النصوص المشفرة- مازالت تحت التطوير، من قبل منظمات المعايير الدولية. ومن المتوقع أن يتم اختيار تصاميم التشفير المبنية على الشبكات (Lattice-based Schemes) مثل Brakerski-Gentry-Vaikuntanathan (BGV)، Brakerski-Fan-Vercauteren (BFV) و Gentry-Sahai-Waters (GSW) بوصفها تصاميم معتمدة للتشفير المتشاكل بالكامل (FHE). أما التشفير المتشاكل الجزئي (Partially Homomorphic Encryption, PHE) الذي يتيح عمليات محدودة على البيانات المشفرة؛ فيدعم عادة إما الجمع أو الضرب. وقد اعتمدت الوثيقة ISO/IEC 18033-6:2019 التصميمين Paillier و Exponential Elgamal كتصاميم تشفير متشاكلة جزئياً (PHE).

٢- الحوسبة متعددة الأطراف Multi-Party Computation (MPC)

الحوسبة متعددة الأطراف هي فرع من فروع التشفير، تتيح فيه التصاميم لعدّة أطراف، حساب دالّة على مدخلاتهم، مع إبقاء مدخل كل طرف سرّا. ويتيح ذلك للمشاركين معرفة الناتج النهائي للحساب، من دون كشف مدخلاتهم الخاصة للآخرين. توجد جهود متعددة من قبل منظمات المعايير العالمية؛ لإصدار معايير لهذه التصاميم، مثل سلسلة ISO/IEC 4922 إذ يضع الجزء الأول المصطلحات العامة، ونماذج الأمان؛ لضمان التشغيل البيني (Interoperability). ويُفصِّل الجزء الثاني آليات لتقاسم السر (Secret Sharing). وقد أطلقت NIST عبر NISTIR 8214C النداء الأول لجمع تصاميم التشفير الحدية متعددة الأطراف (Multi-Party Threshold Schemes) ليتم الاعتماد عليها في تطوير المجال.

٣- الإثبات بلا كشف Zero-Knowledge Proofs (ZKPs)

الإثبات بلا كشف (Zero-knowledge proof, ZKP) هو تصميم من تصاميم التشفير، يتيح لطرفٍ أن يقنع طرف آخر بأن عبارة ما صحيحة؛ من غير أن يكشف أي معلومات، تتجاوز ثبوت صحة العبارة ذاتها. يفيد هذا التصميم في إجراءات التحقق والمصادقة (authentication and validation). تعمل منظمات المعايير العالمية مثل NIST و ISO و ETSI على تطوير معايير لتصاميم الإثبات بلا كشف (ZKPs) لتعزيز أمانها وقابليتها للتشغيل البيني (Interoperability). تشمل جهود NIST جمع تصاميم التشفير متعددة الأطراف؛ وهو جزء أساسي من عملية

محتوى هذا القسم ليس جزءًا من المعايير المُلزم تطبيقها.

تطوير المعايير؛ إذ أن الوثيقة NISTIR 8214C تطلب تقديم تصاميم الإثبات بلا كشف (ZKPs) بالإضافة لتصاميم الحوسبة متعددة الأطراف (MPC). وبالإضافة لما ذكر؛ فإن ISO تطور معايير مثل ISO/IEC 27565 لتكون دليلا إرشاديا لاستعمال تصاميم الإثبات بلا كشف (ZKPs) فيما تستكشف ETSI استخدامها في تطبيقات مثل محافظ الهوية الرقمية (Digital Identity Wallets) من خلال تقارير فنية، مثل ETSI TR 119 476.

الملحق (ب) 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؛ بهدف الوصول للبيانات الحساسة[20]. حيث يمكن تنفيذ هجمات من قبل أعداء غير نشيطين، ويعملون عن بُعد؛ مما يزيد من صعوبة اكتشافهم، وقد يؤدي إلى تسرب مهم، 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[21]. على سبيل المثال، إزالة أي ارتباط بين التمثيل الثنائي للمفتاح السري، وإشارات القناة الجانبية؛ أي باستخدام عمليات وهمية، لإخفاء أي ارتباط محتمل.

التدابير اللازمة لتقليل مخاطر الهجمات الجانبية[٢٢]:

- 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. ويجب الامتناع عن إجراء أي معالجة أخرى للبيانات المشفرة، غير الموثوقة.

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

[20] P. C. Kocher, J. Jaffe and B. Jun, “Differential power analysis,” in Differential power analysis, 2011.

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

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

الملحق (ج) التشفير المبني على السمات Attribute-based Cryptography

التشفير المبني على السمات (Attribute-based Cryptography-ABC) هو نوع من أنواع التشفير بالمفتاح العام (Public-key Cryptography) تشفر فيه البيانات، بحيث يستطيع فكها كل من يملك مجموعة محددة من السمات. يتيح هذا الأسلوب تحكما دقيقا في صلاحيات الوصول. فمثلاً، يمكن تشفير ملف من الملفات بحيث لا يتمكن من الوصول إليه إلا المستخدمون، الذين تتوفر لديهم سمتا (الموارد البشرية) و(مدير). تتناول منظمات المعايير العالمية، مثل NIST في الوثيقتين NIST SP 800-162 و NIST IR 8450 مفهوم التحكم بالوصول القائم على السمات (Attribute-based Access Control-ABAC) على نحوٍ عام. كما تتناول ETSI هذه التقنية في ETSI TS 103 532 التي تُحدِّد التشفير القائم على السمات (ABE) لأغراض التحكم بالوصول القائم على السمات (ABAC) بما يبرز أثره في تأمين الاتصالات والبيانات.

الملحق (د) التشفير المبني على الهوية Identity-based Cryptography

التشفير المبني على الهوية (Identity-based Cryptography, IBC) هو نوع من أنواع التشفير غير المتماثل؛ يكون فيه المفتاح العام سلسلة فريدة (unique string) مرتبطة بهوية المستخدم؛ مثل عنوان البريد الإلكتروني، تنتفي معه الحاجة إلى هيئة شهادات (CA) تربط هوية المستخدم مع مفتاحٍ عام. أما المفتاح الخاص فيجري توليده من قبل جهة مركزية، تعرف بـ مولد المفتاح الخاص (Private-key Generator-PKG). وقد جرى تعريف هذا المفهوم من مفاهيم التشفير في الوثيقة ISO/IEC 18033-5:2015. كما تقدم IETF في RFC 5408 توصيفا لخوارزمية توقيع مبنية على الهوية (Identity-based signature-IBS)، بحيث تبرز تطبيق هذه التقنية في التواقيع الرقمية. وتستعرض الوثيقة NIST IR 8450 المبادئ الأساسية، وحالات استخدام التشفير المبني على الهوية (IBC). إضافةً إلى ذلك، يوفّر التقرير الفني ETSI TR 103 719 دليلاً هندسيًا لاعتماد أنظمة التشفير وتصميمها المبني على الهوية (IBC).

الملحق (هـ) مصطلحات وتعريفات

جدول١: مصطلحات وتعريفات

المصطلح	التعريف
Agility قابلية التحديث	خاصية النظام، أو البنية التحتية، التي من الممكن إعادة تشكيلها، أو إعادة تخصيص الموارد أو إعادة استخدامها، أو توجيهها لأغراض أخرى.
Asymmetric Algorithm خوارزمية غير متماثلة	التشفير الذي يستخدم مفتاحين منفصلين لتبادل البيانات؛ أحدهما لتشفير البيانات، أو توقيعها رقمياً، والآخر لفك تشفير البيانات، أو التحقق من التوقيع الرقمي. وهذا يُعرف أيضًا باسم تشفير المفاتيح العامة.
Authenticated Encryption تشفير موثوق	تحويل البيانات، بواسطة خوارزميات التشفير؛ إلى بيانات مشفرة، لا يمكن تغييرها بواسطة جهة/كيان غير مصرح له/لها من دون اكتشاف التغيير. وهذه العملية توفر سرية البيانات وسلامتها، وتوثيق مصدرها.
Authentication التوثيق	التحقق من هوية المستخدم، أو العملية، أو الجهاز؛ وغالباً ما تكون شرطاً مسبقاً، 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 المتماثلة؛ التي تقسم البيانات إلى مجموعات، أو كتل؛ ثم تقوم بتشفير كل واحدة على حدة.
Blocks of Data كتل البيانات	وحدات من البيانات ذات طول ثابت تكون مدخلات لخوارزميات التشفير؛ أثناء المعالجة، كالنصوص غير المشفرة، ومتجهات التهيئة (IV) أو الأرقام الابتدائية (Nonce) أو البيانات المرتبطة (AD).
Certificate شهادة	مجموعة من البيانات، التي تحدد بصفة فريدة؛ المفتاح العمومي للكيان، والمعلومات الأخرى، التي يجري توقيعها رقميًا، من قبل هيآت الشهادات (أطراف موثوقة). وبهذا الشكل يجرى 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 شهادات المفاتيح العامة للتشفير وإلغائها.
Confidentiality السرية	خاصية منع إتاحة المعلومات، أو الكشف عنها للأفراد، أو الكيانات؛ أو منع إتاحة العمليات غير المصرح لها.
Cryptographic Primitive أساسيات التشفير	خوارزمية تشفير منخفضة المستوى؛ تستخدم بوصفها وحدة بناء أساسية لخوارزميات التشفير، ذات المستويات الأعلى منها.
Cryptographic Solution حلول التشفير	التصاميم والمعمارية، والتنفيذ لأنظمة التشفير ومتطلباته؛ التي جرى اختيارها من قبل الجهات، لتحقق متطلبات تشفيريه محددة.
Cryptography التشفير	المبادئ والوسائل والطرق المؤدية إلى تطبيق خوارزميات تحويل البيانات؛ لأغراض أمنية، تشمل السلامة، والسرية والتوثيق، والموثوقية، ومنع الإنكار.
Cryptosystem نظام التشفير	مجموعة من الخوارزميات والتصاميم، التي تؤدي وظائف التشفير.

المصطلح	التعريف
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.
Decryption فك التشفير	عملية يجري فيها تحويل البيانات المشفرة إلى البيانات الأصلية؛ باستخدام إحدى خوارزميات تقنيات التشفير، والمفتاح الخاص بذلك.
Digital Signature التوقيع الرقمي	هو ناتج تحويل تشفيري للبيانات؛ يتيح عند تنفيذه بالشكل المناسب، التأكد من موثوقية البيانات وسلامتها، ومن ثم منع إنكار الطرف المُوقِّع.
Digital Signature Algorithm (DSA) خوارزمية التوقيع الإلكتروني	خوارزمية يستخدمها الموقِّع لإنشاء توقيع رقمي على البيانات، ويستخدمها 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 إحدى خوارزميات تقنيات التشفير، والمفتاح الخاص بذلك.
End-to-End Encryption تشفير كامل المسار	هي تصاميم تشفير، يتم تشفير البيانات المتبادلة بين أطراف الاتصال؛ ولا يمكن لأي طرف آخر (مثل الخوادم أو أجهزة البنية التحتية للشبكة أو مزودي الخدمات) فك التشفير.
Entropy درجة العشوائية	مقياس لمدى العشوائية التي تواجه المهاجم؛ لتحديد القيمة السرية. ويعبر عنه بوحدات البت. فالقيمة التي تحتوي على n بت من درجة العشوائية، لها الدرجة نفسها في عدم التنبؤ لتوزيع منتظم لـ n بت عشوائياً.
Hardware Security Module (HSM) وحدة أمن الأجهزة	جهاز يضمن سلامة مفاتيح التشفير، وحمايتها، وإدارتها، ومعالجتها. ووحدة أمن الأجهزة، قد تكون وحدة تشفير، أو تحوي على وحدات تشفير.
Hash Function دوال الاختزال	دالة تقوم بتحويل سلسلة أرقام ثنائية (بوحدات البت) ذات طول عشوائي، إلى سلسلة أرقام ثنائية؛ ذات طول ثابت . وغالبًا ما يستحيل إعادة هذا المخرج إلى أصله، ويمثل هذا المخرج صورة مختصرة للمدخلات.
Hash-based MAC (HMAC) رموز توثيق الرسائل المبنية على دوال الاختزال	رموز لتوثيق الرسائل؛ باستخدام دالة اختزال مقبولة، ومفتاح.
Integrated Encryption التشفير المتكامل	تطبيق للتشفير؛ يجمع بين خوارزميتي تشفير أو أكثر. ويتحقق هذا بالذات في الدمج بين التشفير المتماثل (Symmetric Encryption) وغير المتماثل (Asymmetric Encryption).
Hybrid-PRNG مولد أعداد شبه عشوائية هجينة	مولد أعداد شبه عشوائية؛ يستخدم بذرة عشوائية، على أنها مُدخل من مصدر للعشوائية؛ بحيث يكون مولد الأعداد مناسباً لتطبيقات التشفير.
Initialization Vector/ Nonce (IV/Nonce) متجه التهيئة/الرقم الابتدائي	قيمة معلومة تستخدم على أنها مدخل لتهيئة خوارزمية التشفير؛ لرفع مستوى الأمان، ودعم التزامن.
Integrity السلامة	خاصية عدم تغيير البيانات، بصفة غير مصرح بها؛ منذ إنشائها، أو خلال نقلها، أو تخزينها.

المصطلح	التعريف
Invasive Attacks هجمات تدخلية	الهجمات التي تتطلب اتصالاً أو تغييراً مادياً مباشراً، بمكونات التشفير، وهي ما قد تؤدي إلى انحراف في عمليات التشفير؛ مما يسبب تغيراً في عملها الاعتيادي.
Integrity Check Value (ICV) قيمة التحقق من السلامة	ناتج عملية جمع خاصة؛ يمكن من خلاله اكتشاف التعديلات على نظام معلوماتي.
KECCAK خوارزمية اختزال - كاتشاك	عائلة دوال الإسفنج (sponge) مع خاصية التبديل (KECCAK-f) على أنها دالة أساسية. مع الحشو/التعبئة، ذات المعدلات المتعددة؛ لتكون قاعدة للتعبئة.
Key Agreement الاتفاق على المفاتيح	إجراء لإنشاء المفاتيح؛ بحيث تكون مادة المفاتيح الناتجة، متولدة عن دالة تعالج معلومات أُسهمَ بها اثنان، أو أكثر، من المشاركين. على ألا يمكن لأي طرف منهما، تحديد قيمة مادة المفاتيح، باستقلال عن إسهام الأطراف الاخرى.
Key Archival أرشفة المفاتيح	وظيفة في دورة المفاتيح، تتكون من مستودع للتخزين؛ طويل الأجل لمكونات المفاتيح.
Key Derivation Functions (KDFs) دالة اشتقاق المفاتيح	هي العملية التي يجري من خلالها، اشتقاق مفتاح أو أكثر؛ وذلك من خلال مفتاح جرت مشاركته مسبقاً، أو من معلومات سرية، وأخرى مشتركة.
Key Destruction إتلاف المفاتيح	عملية إزالة جميع آثار مادة المفاتيح؛ مما يمنع استردادها بأي وسيلة مادية أو إلكترونية.
Key Exchange تبادل المفاتيح	عملية تبادل المفاتيح العام؛ 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 في عملية التسجيل الرسمي لمكونات المفتاح، بواسطة هيآت الشهادات.
Key Revocation إلغاء المفاتيح	وظيفة ضمن دورة حياة المفتاح؛ يجري 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 / Key Distribution نقل المفاتيح / توزيع المفاتيح	إجراء لتأسيس المفتاح، إذ تقوم إحدى الجهات بنقل المفتاح، وإيصاله إلى جهة أخرى.
Key Wrap (KW) تغليف المفاتيح (حماية المفاتيح)	طريقة لتشفير المفاتيح (تشمل السلامة) توفر السرية والسلامة؛ وذلك باستخدام خوارزمية مفاتيح متماثلة.
Lightweight Cryptography التشفير الخفيف	فئة فرعية في مجال التشفير؛ تهدف إلى توفير حلول أمنية للأجهزة ذات الموارد المحدودة.
Message Authentication Code (MAC) رموز توثيق الرسائل	مجموع اختباري تشفيري للبيانات. يستخدم مفتاحا متماثلاً للكشف عن التعديلات المقصودة، وغير المقصودة على البيانات .كما توفر رموز توثيق الرسائل خاصية الموثوقية والسلامة.
Message Blocks كتل الرسالة	الكتلة الواحدة، الناتجة عن تقسيم الرسالة، إلى كتل بطول 128-بت.

المصطلح	التعريف
Non-Invasive Attacks هجمات غير تدخلية	الهجمات المعتمدة على تسرب المعلومات المادي، من حلول التشفير. وتستهدف بعض الخصائص؛ مثل الوقت المستغرق، والطاقة المستهلكة، والانبعاثات الكهرومغناطيسية، والصوتية.
Non-Repudiation عدم الإنكار	خدمة تستخدم التوقيع الرقمي؛ للتحقق من أن كياناً محدداً قد وقع فعلياً على رسالة محددة؛ فلا يمكنه نفي ذلك.
Online Certificate Status Protocol (OCSP) بروتوكول حال الشهادة عبر الإنترنت	بروتوكول عبر الإنترنت؛ يستخدم لتحديد حال الشهادة للمفتاح العام.
Post-Quantum Cryptography (PQC) التشفير لما بعد الحوسبة الكمية	أنظمة التشفير التي ستكون آمنة ضد الهجمات، باستخدام الحاسب التقليدي، أو الكمي. ويمكن الاستفادة منها؛ دون الحاجة إلى تغيير شبكات التواصل الحالية وبروتوكولاته.
Pre-Shared Key المفتاح المشترك مسبقاً	المفتاح الخاص الذي جرى إنشاؤه بين الأطراف المصرح لهم باستخدامه، وجرى توزيعه بوسائل آمنة (مثل: التوزيع اليدوي بإجراءات آمنة، أو الإنشاء الآمن والتلقائي للمفاتيح).
Private Key مفتاح خاص	في الخوارزمية غير المتماثلة، يجري استخدام المفتاح الخاص للتوقيع الرقمي، وكذلك يفكُ به تشفير البيانات؛ ويجب أن يبقى سريًا.
Pseudo Random Number Generator (PRNG) مولد أعداد شبه عشوائية	مولد أعداد عشوائية، لديه إمكانية الوصول لمصدر عشوائي؛ لإنتاج سلسة من الأرقام الثنائية (بوحدات البت) باستخدام بذرة عشوائية سرية (seed) إلى جانب مدخلات أخرى محتملة.
Public Key مفتاح عام	في الخوارزمية غير المتماثلة، يجري استخدام المفتاح العام؛ للتحقق من التوقيع الرقمي، وكذلك لتشفير البيانات؛ ويكون معروفاً للعموم.
Public Key Infrastructure (PKI) البنية التحتية للمفاتيح العامة	إطار يجري إنشاؤه لإصدار شهادات المفاتيح العامة، وحفظها وإلغائها.
Quantum Computing الحوسبة الكمية	تقنية حديثة، تعتمد على قوانين الفيزياء الكمية؛ لحل المشكلات المعقدة جداً على التقنية الحاسوبية الحالية.
Quantum Cryptography (QC) التشفير الكمي	حلول تشفير، تعتمد على قوانين الفيزياء الكمية؛ لتقديم أنظمة أمنية معينة.
Quantum Key Distribution (QKD) توزيع المفاتيح الكمي	طريقة آمنة لتبادل المفاتيح، تعتمد على قوانين الفيزياء الكمية، بدلاً من العمليات الحاسوبية الحالية ذات التعقيد الشديد.
Quantum Random Number Generation (QRNG) توليد الأعداد الكمية العشوائية	توليد أعداد تامة العشوائية؛ باستخدام مصادر ذات درجة عالية في العشوائية؛ تعتمد على خاصية عدم القدرة على التنبؤ، المرتبطة بالفيزياء الكمية.
Random Number Generator (RNG) مولد أعداد عشوائية	عملية توليد سلسلة عشوائية من القيم (في الغالب سلسلة من الأرقام الثنائية - بت) أو قيمة عشوائية واحدة.
Root Certificate الشهادات الجذرية	يجري تنصيب الشهادة الجذرية في الأنظمة، بطريقة آمنة؛ حتى تتمكن من توثيق شهادات المستخدمين النهائيين.
RSA	خوارزمية غير متماثلة تستخدم لإنشاء المفاتيح، وتوليد التوقيع الرقمي، والتحقق منه.

المصطلح	التعريف
Safe Primes أعداد أولية آمنة	يقال عن العدد الأولي p آمن إذا كان $p = 2q + 1$ بحيث أن q عدد أولي. ويجب استخدام مولد برتبة عالية (large order generator).
Secret Key مفتاح سري	مفتاح تشفير، يستخدم بواسطة خوارزميات التشفير (المتماثلة) ولا يسمح بنشره، ولا استخدامه، من قبل الجهات غير المصرح لها بذلك. ويسمى أيضاً بالمفتاح المتماثل (symmetric key).
Security Level مستوى الأمان	رقم يحدد مقدار العمليات الحسابية المُتوقعة؛ لكسر منظومة تشفير (كتعطيل وظائفه أو حمايته). ويقاس مستوى الأمان بالبيانات الثنائية – بت. فإذا كان مستوى أمان المنظومة n بت؛ فمن المتوقع أن يتطلب كسرها 2^n عملية معينة.
Seed بذرة العشوائية	قيمة لمُدخل ابتدائي سري، لمولد الأعداد شبه العشوائية. إذ إن بذرات العشوائية المختلفة، مع مدخلات محتملة أخرى؛ تنشئ سلاسل أرقام شبه عشوائية مختلفة.
Stream Cipher Algorithm خوارزمية التشفير الانسيابية	طريقة تشفير بالمفتاح المتماثل. بحيث 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 تُعرَّف 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 مفتاحاً سرياً واحداً، لكل من عمليتي التشفير، وفك التشفير.
True Random Number Generator (TRNG) مولد الأعداد تامة العشوائية	مولد أرقام عشوائية، لديه القدرة على الوصول الدائم لمصدر العشوائية. وعند عمله بشكل صحيح؛ ينتج مخرجاً ذا عشوائية تامة.

الملحق (و) قائمة الاختصارات

جدول٢: قائمة الاختصارات

الاختصار	المعنى
AEAD	Authenticated Encryption with Associated Data التشفير والتوثيق، باستخدام البيانات المرتبطة
AES	Advanced Encryption Standards معيار التشفير المتقدم.
ALIKE	Authenticated Lightweight Key Exchange تبادل المفاتيح الخفيفة والموثقة.
ARLs	Authority Revocation Lists قوائم الهيآت 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.
cSHAKE	customizable Secure Hash Algorithm with KECCAK خوارزمية اختزال معدلة باستخدام كاتشاك (KECCAK).
CTR	Counter 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.

الاختصار	المعنى
ECDLP	Elliptic Curve Discrete Logarithm Problem اللوغاريثم المتقطع، للمنحنى الإهليجي.
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.
E2EE	End-to-End Encryption تصاميم تشفير كامل المسار
ETSI	European Telecommunications Standards Institute المعهد الأوربي لمعايير الاتصالات.
FIPS	Federal Information Processing Standards معايير عمليات المعلومات الفيدرالية.
GCM	Galois Counter Mode طريقة استخدام عداد Galois للتشفير والتوثيق؛ باستخدام البيانات المرتبطة.
GMAC	Galois Message Authentication Code رموز توثيق الرسائل، المبنية على عداد Galois.
GS QKD	Group Specification Quantum Key Distribution توزيع المفتاح الكمي لمواصفات المجموعة.
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.
HSM	Hardware Security Module وحدة أمن الأجهزة.
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.

الاختصار	المعنى
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission المنظمة الدولية للمعايير /اللجنة الكهروتقنية الدولية.
IT	Information Technology تقنية المعلومات.
IV	Initialization Vector متجه التهيئة.
KDF	Key Derivation Functions دوال اشتقاق المفاتيح.
KLM	Key Lifecycle Management إدارة دورة المفاتيح.
KMAC	KECCAK Message Authentication Code رموز توثيق الرسائل باستخدام كاتشاك (KECCAK).
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.
NIST	National Institution of Standard and Technology المعهد الوطني للمعايير والتقنية.
NIST SP	National Institution of Standard and Technology Special Publication إصدار خاص للمعهد الوطني للمعايير والتقنية.
OCSP	Online Certificate Status Protocol بروتوكول حال الشهادة عبر الإنترنت.
OFB	Output Feedback التغذية الراجعة للمخرجات (إحدى عمليات التشفير).
PKI	Public Key Infrastructure البنية التحتية للمفاتيح العامة.
PQC	Post-quantum Cryptography الحوسبة لما بعد الكمية.
PRNG	Pseudo Random Number Generator مولد الأعداد شبه العشوائية.
QKD	Quantum Key Distribution توزيع المفتاح الكمي.
QRNG	Quantum Random Number Generator مولد الأعداد العشوائية الكمية

الاختصار	المعنى
RNG	Random Number Generator مولد الأعداد العشوائية.
RSA	Algorithm Developed by Rivest, Shamir and Adelman خوارزمية جرى 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.
SHAKE	Secure Hash Algorithm with KECCAK خوارزمية اختزال باستخدام كاتشاك (KECCAK).
SSH	Secure Shell الاتصال الآمن عن بعد.
TLS	Transport Layer Security بروتوكول طبقة النقل الآمنة.
TRNG	True Random Number Generator مولد أعداد عشوائية.
UEA	Universal Mobile Telecommunications System 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.

الملحق (ز) قائمة التحديثات

جدول٣: قائمة التحديثات

النسخة			التاريخ
NCS – 2			2025
نوع التحديث	القسم	الصفحة	الوصف
تعديل	النطاق	٨	توضيح الأقسام المضافة.
إضافة	النطاق	٨	توضيح مستوى الأمان المستهدف لنظم التشفير.
تعديل	٣-١	٩	توضيح الأقسام المضافة.
حذف	٢-١	١٠	حذف العنوان.
تعديل	٢-١-٣	١١	إعادة صياغة.
تعديل	٢-٣-١	١١	تعديل لإضافة SHA2-256 و SHA2-512، وإعادة صياغة المعيار.
تعديل	٢-٣-٣	١١	إعادة صياغة.
تعديل	٢-٤	١١	تغيير العنوان.
تعديل	٢-٤-٢	12	إعادة صياغة وإضافة متطلبات جديدة.
إضافة	٢-٥	١٢	إضافة معايير جديدة لخوارزميات ما بعد الحوسبة الكمية.
حذف	٢-٥-٣	١٢	نُقل للحاشية
إضافة	٢-٦-٦	١٣	إضافة معايير جديدة لخوارزمية Ascon.
تعديل	٣	١٤	حذف الملاحظة العامة والاكتفاء بـ٣-١-٢.
تعديل	٣-١-١	١٤	إعادة صياغة.
تعديل	٣-١-٢	١٤	إعادة صياغة.
تعديل	٣-١-٣	١٤	إعادة صياغة.
تعديل	٣-١-٦	١٤	إضافة متطلبات جديدة لطرق عمليات التشفير.
تعديل	٣-٢-١	١٤	إعادة صياغة.
تعديل	٣-٢-١-١	١٤	تعديل طول متجه التهيئة/متجه التهيئة (IV) إلى 128-بت.
تعديل	٣-٢-١-٢	١٤	إعادة صياغة.
إضافة	٣-٢-١-٤	١٤	إضافة متطلبات جديدة.
إضافة	٣-٢-٢	١٤	إضافة متطلبات جديدة.
تعديل	٣-٣	١٥	إعادة صياغة.
تعديل	٣-٣-١-١	١٥	إضافة متطلبات جديدة.
إضافة	٣-٣-٢-١	١٥	إضافة متطلبات جديدة.
تعديل	٣-٣-٢-٤	١٥	تعديل طول الوسم إلى 128-بت
إضافة	٣-٣-٣	١٥	إضافة معايير جديدة لـKMAC
إضافة	٣-٣-٤	١٥	إضافة معايير جديدة لـGMAC
تعديل	٣-٦-٣	١٦	إعادة صياغة.

تعديل	٣-٧	١٧	تغيير العنوان
تعديل	٣-٧-٢	١٧	إعادة صياغة.
تعديل	٣-٧-٣	١٧	إعادة صياغة.
تعديل	٣-٨	١٧	تغيير عنوان
تعديل	٣-٨-٢	١٧	إعادة صياغة.
تعديل	٤-١	١٩	إعادة صياغة.
تعديل	٤-٢-٢	٢٠	إعادة صياغة.
تعديل	٤-٢-٣	٢٠	إعادة صياغة.
تعديل	٤-٢-٤	٢٠	إعادة صياغة.
تعديل	٤-٧	٢٢	حذف الملاحظة العامة والاكتفاء بـ٤-٧-١
تعديل	٦-٢-١	٢٥	إعادة صياغة.
تعديل	٦-٢-٢-٢	٢٥	إعادة صياغة.
تعديل	٦-٢-٢-٣	٢٥	إعادة صياغة.
إضافة	٦-٣-٢-٦	٢٦	إضافة متطلبات جديدة.
إضافة	٦-٢-٥-١	٢٦	إضافة متطلبات جديدة.
تعديل	٦-٢-٨-٢	٢٦	تغيير المرجع.
تعديل	٦-٢-٩-٣	٢٦	إعادة صياغة.
إضافة	٦-٢-١٠-١	٢٧	إضافة متطلبات جديدة.
إضافة	٧	٢٨	إضافة متطلبات جديدة لمولدات الأعداد العشوائية (RNGs)
إضافة	٨	٢٩	إضافة متطلبات جديدة للتوزيع الكمي لمفاتيح التشفير (QKD)

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority