أساسيات التشفير

د/ خالد السيد عبد الحق

د/ دعاء محمود عبدالعال

جدول المحتويات

الفصل الأول: مقدمة في علم التشفير ٧
تعريف التشفير وأهميته ١٠
تاريخ التشفير وتطوره ٢٠
الفرق بين التشفير الكلاسيكي والتشفير الحديث ٣٢
المبادئ الأساسية للأمان في التشفير (السرية، النزاهة، المصادقة) ٣٥
الفصل الثاني: أنظمة التشفير المتماثل ٤٣
مفهوم التشفير بالمفتاح الواحد ٤٦
خوارزميات التشفير التقليدية ٦٠
خوارزمية التشفير AES ومعاييرها ٦٦
أنماط تشغيل التشفير المتماثل (ECB, CBC, CFB, OFB, CTR) ٨٤
نقاط القوة والضعف في أنظمة التشفير المتماثل ٩٠
الفصل الثالث: أنظمة التشفير غير المتماثل ٩٣
مفهوم التشفير بالمفتاح العام والخاص ٩٦
خوارزمية "RSA": البنية والآلية والتطبيقات ٩٨
تبادل المفاتيح باستخدام "ديفي-هيلمان" ١٠٦
تشفير المنحنيات البيضاوية (Elliptic Curve Cryptography - ECC) ١١١
الفصل الرابع: دوال الهاش والتكاملية ١١٥
مفهوم دوال الهاش وأهميتها ١١٨
خصائص دوال الهاش المثالية ١٢٣
أشهر خوارزميات الهاش (MD5, SHA-1, SHA-2, SHA-3) ١٣٥
تطبيقات دوال الهاش في التحقق من سلامة البيانات ١٤٤
الفصل الخامس: المصادقة والتوقيعات الرقمية ١٤٩
أهمية المصادقة في الأنظمة المشفرة ١٥٢
التوقيعات الرقمية: المفهوم وآلية العمل ١٥٦
البنية التحتية للمفتاح العام (PKI) ودورها في المصادقة ١٦٠
شهادات التصديق الإلكتروني وسلطات التصديق ١٦٥
الفصل السادس: توليد الأرقام شبه العشوائية وأمان المفاتيح ١٦٩
أهمية العشوائية في التشفير ١٧٢
الفارق بين الأرقام العشوائية والحتمية ١٧٩
خوارزميات توليد الأرقام العشوائية (PRNG, CSPRNG) ١٨١

أمن المفاتيح وإدارتها ١٨٤
الفصل السابع: البروتوكولات الأمنية والتشفير في التطبيقات العملية ١٨٧
أساسيات البروتوكولات الأمنية ١٩٠
بروتوكولات المصادقة ١٩٦
بروتوكولات الاتصال المشفر ١٩٨
تطبيقات التشفير في الحوسبة السحابية والبلوك تشين ٢٠١
الفصل الثامن: تحليل أمان التشفير والهجمات الشائعة **٢٠٩**
تصنيف الهجمات على أنظمة التشفير ٢١٢
هجمات القوة الغاشمة (Brute Force) وتحليل التردد ٢١٤
هجمات الشخص في المنتصف (MITM) ٢١٩
الهجمات الجانبية (Side-Channel Attacks) ٢٢١
الفصل التاسع: مستقبل التشفير والتحديات القادمة **٢٢٥**
تأثير الحوسبة الكمية على أنظمة التشفير ٢٢٨
تطوير خوارزميات مقاومة للحوسبة الكمية ٢٣٠
الاتجاهات الحديثة في أمن المعلومات ٢٣٣
تطبيقات عامة ٢٣٧

مقدمة

في العصر الرقمي الذي نعيشه اليوم، أصبح تأمين البيانات والمعلومات من أهم التحديات التي تواجه الأفراد والمؤسسات على حد سواء. فمع التوسع الهائل في استخدام الإنترنت والتكنولوجيا الحديثة، ازدادت الحاجة إلى وسائل تضمن سرية المعلومات وحمايتها من التلاعب أو الاختراق. وهنا يأتي علم التشفير ليشكل الركيزة الأساسية في تأمين البيانات وضمان خصوصيتها.

يُعرف التشفير بأنه العلم الذي يهتم بتحويل المعلومات إلى شكل غير مفهوم أو مشفر بحيث لا يمكن قراءته إلا من قبل الأطراف المصرح لهم بذلك. ومنذ القدم، استخدم البشر التشفير لحماية الرسائل والمعلومات الحساسة، بدءًا من الأساليب البدائية في العصور القديمة وحتى الخوارزميات المعقدة التي نشهدها اليوم. فقد تطور علم التشفير من مجرد استبدال الأحرف والرموز إلى أنظمة تعتمد على الرياضيات المتقدمة والخوارزميات المعقدة التي توفر مستويات عالية من الأمان.

يهدف هذا الكتاب إلى تقديم فهم شامل لمبادئ التشفير وأساسياته، بحيث يكون مرجعًا للطلاب والباحثين وكل من يهتم بمجال أمن المعلومات. يتناول الكتاب في فصوله المختلفة تطور علم التشفير، بدءًا من الأساليب التقليدية ووصولًا إلى التشفير الحديث المستخدم في تأمين البيانات الإلكترونية والتواصل الرقمي. كما يناقش الكتاب أنظمة التشفير المتماثل وغير المتماثل، ودوال الهاش، والمصادقة الرقمية، بالإضافة إلى التطبيقات العملية للتشفير في الحياة اليومية.

إن فهم علم التشفير لا يقتصر على المختصين في مجال أمن المعلومات فقط، بل هو أمر ضروري لكل مستخدم للتكنولوجيا، سواء كان ذلك في المعاملات المالية عبر الإنترنت، أو حماية البيانات الشخصية، أو حتى في التطبيقات الحديثة مثل تقنية البلوك تشين والحوسبة السحابية. لذلك، يسعى هذا الكتاب إلى تقديم محتوى علمي بأسلوب مبسط يساعد القارئ على استيعاب المفاهيم الأساسية واستكشاف الجوانب العملية لهذا العلم الحيوي.

نأمل أن يكون هذا الكتاب دليلاً مفيدًا لكل من يرغب في التعرف على علم التشفير وأهميته، وأن يساهم في نشر الوعي بأهمية حماية البيانات في العالم الرقمي الحديث.