Cyber Security and Technology

Data Encryption Mastery Deep Dive into Cybers

Code: 259010

FUTURE CENTRE
مركز المستقبل

futurecentre.net

Course Introduction

In an era of pervasive data breaches and sophisticated cyber threats, encryption is the last line of defense—the unbreachable vault for your most critical digital assets. However, simply implementing encryption is not enough. Misconfigured algorithms, poor key management, and a misunderstanding of cryptographic fundamentals can create a false sense of security.

This advanced, technical deep-dive moves beyond the high-level overviews to explore the mathematical foundations, operational mechanisms, and practical implementation of modern cryptography. Through rigorous theory and hands-on labs, participants will deconstruct cryptographic algorithms, build secure encryption systems, and learn to exploit common vulnerabilities. This course is designed for those who don't just want to use encryption, but to truly master it.

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a binder containing a copy of the presentation
- slides and handouts
- Post-assessment

Course Objectives

Upon successful completion of this course, participants will be able to:

- **Explain** the core mathematical concepts (modular arithmetic, prime numbers, elliptic curves) that underpin modern cryptography.
- **Differentiate** between and implement symmetric, asymmetric, and hybrid cryptosystems, selecting the right tool for a given use case.
- **Design** and **execute** a robust cryptosystem with a secure Key Management Lifecycle (generation, storage, distribution, rotation, destruction).
- **Analyze** and **break** weak cryptographic implementations through hands-on cryptanalysis techniques.
- **Implement** encryption for data in transit (TLS) and data at rest (disk, database) in enterprise environments.
- **Evaluate** the security and trade-offs of various cryptographic standards (AES, RSA, ECC, SHA, Post-Quantum finalists).

Who Should Attend?

This master-level course is designed for technical professionals who design, implement, audit, or manage systems that rely on encryption.

- **Security Architects** & **Cryptographic Engineers**
- **DevSecOps Engineers** & **Software Developers** building security-critical applications
- **Cloud Security Specialists** implementing encryption in IaaS, PaaS, and SaaS
- **Senior System Administrators** & **Network Engineers** responsible for PKI and TLS
- **Security Consultants** & **Penetration Testers** specializing in app security
- **IT Auditors** & **GRC Professionals** who need a deep technical understanding of crypto controls

Prerequisites: A strong comfort with technical concepts and logical reasoning is essential. Familiarity with programming (Python helpful but not mandatory), networking, and basic Linux command line is strongly recommended.

Course Outline

Day 1: Foundations of the Cryptographic Science

- **Module 1: The History and Pillars of Security**
  - Cryptography vs. Cryptanalysis, historical ciphers (Caesar, Vigenère), and the lessons learned.
  - The CIA Triad (Confidentiality, Integrity, Availability) and how cryptography serves them.
- **Module 2: Core Mathematical Concepts**
  - Modular arithmetic, prime numbers, entropy, and one-way functions.
  - Introduction to number theory for public-key crypto.
- **Hands-On Lab:** Breaking classical ciphers with Python scripts and frequency analysis.

Day 2: Symmetric Cryptography & Hashes

- **Module 3: Stream and Block Ciphers**
  - Operational modes (ECB, CBC, GCM), strengths, and weaknesses.
  - Deep dive into the AES algorithm.
- **Module 4: Cryptographic Hash Functions**
  - Properties of cryptographic hashes (SHA-2, SHA-3).
  - Applications: password hashing, digital fingerprints, HMAC.
- **Hands-On Lab:** Implementing AES in different modes; observing patterns in ECB; creating and breaking weak password hashes.

Day 3: Asymmetric Cryptography & Key Management

- **Module 5: Public Key Infrastructure (PKI)**
  - Deep dive into RSA and Elliptic Curve Cryptography (ECC).
  - Diffie-Hellman Key Exchange and the discrete log problem.
- **Module 6: The Key to it All: Key Management**
  - The full key management lifecycle: generation, exchange, storage, rotation, revocation, and destruction.
  - Introduction to HSMs (Hardware Security Modules) and cloud KMS (Key Management Services).
- **Hands-On Lab:** Generating RSA keys, performing encryption/signatures, and simulating a man-in-the-middle attack to break weak key exchange.

Course Outline

Day 4: Applied Cryptography in the Enterprise

- **Module 7: Encryption for Data in Transit**
  - Deconstructing the TLS handshake (1.2 vs. 1.3).
  - Cipher suite negotiation and common misconfigurations.
- **Module 8: Encryption for Data at Rest**
  - Full Disk Encryption (FDE) vs. File-Level Encryption.
  - Application-layer encryption and tokenization for databases.
- **Hands-On Lab:** Using tools like openssl and Wireshark to analyze TLS connections; configuring Apache/Nginx with strong cipher suites.

Day 5: Advanced Topics and the Future

- **Module 9: Cryptanalysis and Common Vulnerabilities**
  - Identifying and exploiting weak implementations: padding oracle attacks, weak randomness, side-channel attacks.
- **Module 10: The Quantum Future**
  - Introduction to Quantum Computing and its threat to current crypto (Shor's Algorithm).
  - Overview of Post-Quantum Cryptography (PQC) and NIST's finalists.
- **Capstone Challenge:** A comprehensive lab where participants must audit, exploit, and then fix a vulnerable application that uses multiple layers of cryptography.
- **Course Recap and The Path Forward**

المقدمة

في عصرٍ تكثر فيه خروقات البيانات والتهديدات السيبرانية المعقدة، يُعد التشفير خط الدفاع الأخير، فهو بمثابة خزنةٍ منيعةٍ لأهم أصولك الرقمية. ومع ذلك، فإن مجرد تطبيق التشفير لا يكفي. فالخوارزميات الخاطئة، وسوء إدارة المفاتيح، وسوء فهم أساسيات التشفير، كلها عوامل قد تُولّد شعورًا زائفًا بالأمان.
يتجاوز هذا التعمق التقني المتقدم النظريات العامة رفيعة المستوى لاستكشاف الأسس الرياضية وآليات التشغيل والتطبيق العملي للتشفير الحديث. من خلال نظريات دقيقة ومختبرات عملية، سيتمكن المشاركون من تحليل خوارزميات التشفير، وبناء أنظمة تشفير آمنة، وتعلم كيفية استغلال الثغرات الأمنية الشائعة. صُممت هذه الدورة لمن لا يرغبون في استخدام التشفير فحسب، بل في إتقانه تمامًا.

طريقة التدريب

- التقييم المسبق
- تدريب جماعي مباشر
- استخدام أمثلة واقعية ودراسات حالة وتمارين
- مشاركة ونقاش تفاعلي
- عرض تقديمي باستخدام باور بوينت، وشاشة LCD، ولوح ورقي
- أنشطة واختبارات جماعية
- يحصل كل مشارك على ملف يحتوي على نسخة من العرض التقديمي
- شرائح ومطبوعات
- التقييم اللاحق

أهداف الدورة

عند إكمال هذه الدورة بنجاح، سيكون المشاركون قادرين على:

- **اشرح** المفاهيم الرياضية الأساسية (الحسابات المعيارية، الأعداد الأولية، المنحنيات الإهليلجية) التي تدعم التشفير الحديث.
- **التمييز** بين أنظمة التشفير المتماثلة وغير المتماثلة والهجينة وتنفيذها، واختيار الأداة المناسبة لحالة استخدام معينة.
- **تصميم** وتنفيذ نظام تشفير قوي مع دورة حياة إدارة مفاتيح آمنة (التوليد والتخزين والتوزيع والتدوير والتدمير) .
- **تحليل** وكسر تنفيذات التشفير الضعيفة من خلال تقنيات تحليل **الشفرات** العملية.
- **تنفيذ** التشفير للبيانات أثناء النقل (TLS) والبيانات في حالة السكون (القرص، قاعدة البيانات) في بيئات المؤسسة.
- **تقييم** الأمان والمقايضات بين معايير التشفير المختلفة (AES، RSA، ECC، SHA، المعايير النهائية لما بعد الكم).

من ينبغي أن يهتم؟

تم تصميم هذه الدورة التدريبية على مستوى الماجستير للمحترفين التقنيين الذين يقومون بتصميم أو تنفيذ أو تدقيق أو إدارة الأنظمة التي تعتمد على التشفير.

- **مهندسو الأمن** ومهندسو **التشفير**
- **مهندسو DevSecOps** ومطورو **البرامج الذين** يقومون ببناء تطبيقات ذات أهمية أمنية
- **متخصصون في أمن السحابة** ينفذون التشفير في SaaSg PaaSg IaaS
- **كبار مسؤولي النظام** ومهندسي **الشبكات** المسؤولين عن TLSg PKI
- **مستشارو الأمن** واختبارات **الاختراق** المتخصصة في أمان التطبيقات
- **مدققو تكنولوجيا المعلومات** ومحترفو **الحوكمة والمخاطر والحوكمة** الذين يحتاجون إلى فهم تقني عميق لضوابط التشفير

المتطلبات الأساسية: إلمام جيد بالمفاهيم التقنية والتفكير المنطقي ضروري. يُنصح بشدة بالإلمام بالبرمجة (بايثون مفيد ولكنه ليس إلزاميًا)، والشبكات، وأساسيات سطر أوامر لينكس

محتويات الكورس

اليوم الأول أساسيات علم التشفير

- **الوحدة 1: تاريخ وركائز الأمن**
  - التشفير مقابل تحليل الشفرات، والشفرات التاريخية (قيصر، فيجينير)، والدروس المستفادة.
  - ثلاثية وكالة المخابرات المركزية (السرية والنزاهة والتوافر) وكيف تخدمها التشفير.
- **الوحدة 2: المفاهيم الرياضية الأساسية**
  - الحساب المعياري، والأعداد الأولية، والإنتروبيا، والدوال أحادية الاتجاه.
  - مقدمة لنظرية الأعداد للتشفير بالمفتاح العام.
- **مختبر عملي:** كسر الشفرات الكلاسيكية باستخدام نصوص بايثون وتحليل التردد.

اليوم الثاني التشفير المتماثل والتجزئة

- **الوحدة 3: التشفير التدفقي والكتلي**
  - الأوضاع التشغيلية (ECB، CBC، GCM)، نقاط القوة والضعف.
  - الغوص العميق في خوارزمية AES.
- **الوحدة 4: وظائف التجزئة التشفيرية**
  - خصائص التجزئات التشفيرية (SHA-2، SHA-3).
  - التطبيقات: تجزئة كلمة المرور، بصمات الأصابع الرقمية، HMAC.
- **مختبر عملي:** تنفيذ AES في أوضاع مختلفة؛ مراقبة الأنماط في ECB؛ إنشاء وكسر تجزئات كلمات المرور الضعيفة.

اليوم الثالث التشفير غير المتماثل وإدارة المفاتيح

- **الوحدة 5: البنية التحتية للمفتاح العام (PKI)**
  - الغوص العميق في RSA والتشفير المنحني الإهليلجي (ECC).
  - تبادل مفتاح ديفي-هيلمان ومشكلة السجل المنفصل.
- **الوحدة 6: مفتاح كل شيء: إدارة المفاتيح**
  - دورة إدارة المفاتيح الكاملة: التوليد، والتبادل، والتخزين، والتدوير، والإلغاء، والتدمير.
  - مقدمة عن وحدات أمان الأجهزة (HSM) وخدمات إدارة المفاتيح السحابية (KMS).
- **مختبر عملي:** إنشاء مفاتيح RSA، وإجراء التشفير/التوقيعات، ومحاكاة هجوم الرجل في المنتصف لكسر تبادل المفاتيح الضعيف.

محتويات الكورس

اليوم الرابع التشفير التطبيقي في المؤسسة

- **الوحدة 7: تشفير البيانات أثناء النقل**
  - تفكيك مصافحة TLS (1.2 مقابل 1.3).
  - التفاوض على مجموعة التشفير والأخطاء الشائعة في التكوين.
- **الوحدة 8: تشفير البيانات الساكنة**
  - تشفير القرص الكامل (FDE) مقابل التشفير على مستوى الملف.
  - تشفير طبقة التطبيق وتجزئة قواعد البيانات.
- **مختبر عملي:** استخدام أدوات مثل Wireshark openssl لتحليل اتصالات TLS؛ وتكوين Apache/Nginx مع مجموعات تشفير قوية.

اليوم الخامس المواضيع المتقدمة والمستقبل

- **الوحدة 9: تحليل الشفرات والثغرات الأمنية الشائعة**
  - تحديد واستغلال التنفيذات الضعيفة: هجمات أوراكل الحشو، والعشوائية الضعيفة، وهجمات القناة الجانبية.
- **الوحدة 10: المستقبل الكمي**
  - مقدمة عن الحوسبة الكمومية وتهديدها للعملات المشفرة الحالية (خوارزمية شور).
  - نظرة عامة على التشفير ما بعد الكم (PQC) والمرشحين النهائيين لجائزة NIST.
- **تحدي Capstone:** مختبر شامل حيث يتعين على المشاركين التدقيق والاستغلال ثم إصلاح تطبيق ضعيف يستخدم طبقات متعددة من التشفير.
- **ملخص الدورة والطريق إلى الأمام**

Terms & Conditions

Complete & Mail to future centre or email

Info@futurecentre.com

Cancellation and Refund Policy

Delegates have 14 days from the date of booking to cancel and receive a full refund or transfer to another date free of charge. If less than 14 days' notice is given, then we will be unable to refund or cancel the booking unless on medical grounds. For more details about the Cancellation and Refund policy, please visit
https://futurecentre.net/

Registration & Payment

Please complete the registration form on the course page & return it to us indicating your preferred mode of payment. For further information, please get in touch with us

Course Materials

The course material, prepared by the future centre, will be digital and delivered to candidates by email

Certificates

Accredited Certificate of Completion will be issued to those who attend & successfully complete the programme.

Travel and Transport

We are committed to picking up and dropping off the participants from the airport to the hotel and back.

Registration & Payment

Complete & Mail to future centre or email

Info@futurecentre.com

Registration Form

- Full Name (Mr / Ms / Dr / Eng) .....
- Position .....
- Telephone / Mobile .....
- Personal E-Mail .....
- Official E-Mail .....
- Company Name .....
- Address .....
- City / Country .....

Payment Options

- ☐ Please invoice me
- ☐ Please invoice my company

Course Calander:

- 09/03/2026 - 13/03/2026 Click Now
- 27/07/2026 - 31/07/2026 Click Now
- 14/12/2026 - 18/12/2026 Click Now

VENUES

- LONDON
- BARCELONA
- KUALA LUMPER
- AMSTERDAM
- DAMASCUS
- ISTANBUL
- SINGAPORE
- PARIS
- DUBAI

OUR PARTNERS

THANK YOU

CONTACT US

+963 112226969

+963 953865520

Info@futurecentre.com

Damascus - Victoria - behind Royal Semiramis hotel

FUTURE CENTRE
مركز المستقبل

futurecentre.net