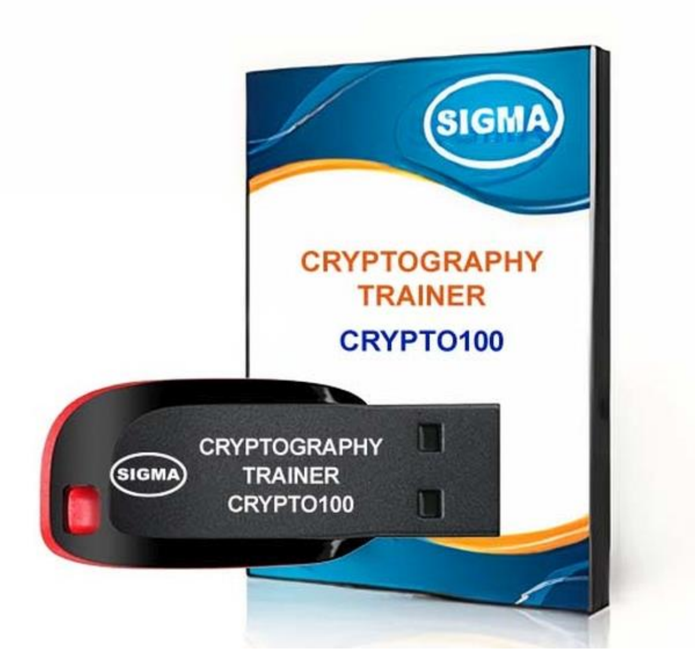
SIGMA

CRYPTOGRAPHY TRAINER
MODEL-CRYPTO100

This Cryptography trainer has been designed with a view to provide practical and experimental knowledge of Cryptography used in Cryptocurrencies like Bit coin.

SPECIFICATIONS



EXPERIMENTS

A. Introduction to Cryptography

1. Information security and cryptography
2. Backgrounds and functions
3. Cryptography Definitions
4. Terminology
5. Cryptography Services
6. Confidentiality (secrecy)
7. Integrity (anti-tampering)
8. Authentication

B. Components of a Basic Cryptosystem

9. Plaintext
10. Encryption Algorithm
11. Ciphertext
12. Decryption Algorithm
13. Encryption Key
14. Decryption Key
15. Digital signatures
16. Authentication and identification
17. Public key cryptography

C. Types of Cryptography

18. Symmetric Key Cryptography
19. Asymmetric Key Cryptography
20. Hash Functions

D. Symmetric (Private Key) Encryption

21. Symmetric encryption schemes
22. Modern stream ciphers
23. Block ciphers
24. Symmetric key distribution
25. Key management
26. Secret key distribution
27. Formal approaches to protocol checking
28. Message authentication codes

E. Asymmetric Encryption

29. Asymmetric encryption schemes
30. Notions of security
31. Hybrid encryption

F. PKI and Encryption

32. Concept of public key infrastructure (PKI)
33. Basic definitions before PKI
34. Public key crypto
35. Certificate
36. Certificate authority
37. Relationship between PKI and basic terms

G. Hash Functions and Data Integrity

38. Introduction to hash functions
39. Classification of hash functions
40. General classification
41. Basic properties of hash functions
42. Iterated hash functions
43. Formatting and initialization of hash functions

H. Digital Signature

44. Introduction to digital signatures
45. Basic definition
46. Digital signature schemes
47. Types of attacks on signature schemes
48. RSA and related signature schemes
49. Possible attacks on RSA signature
50. The Rabin public key signature scheme
51. ISO/IEC 9796 formatting

I. Digital Certificate

52. Definition of digital certificate
53. CA’s identity
54. Owner’s identity
55. Owner’s public key

56. Certificate expiration date
57. CA’s signature for certificate
58. Types of digital certificate
59. Identity certificates
60. Accreditation certificates
61. Authorization and permission certificates
62. Parties to digital certificate
63. Public and private keys
64. Certificate validation
65. 509 certificate
66. Third party digital signature certification authorities
67. New certificate research
68. Companies providing digital certificate
69. RSA
70. Thawte
71. Verisign

J. Cryptographic Threats and Tools

72. Impersonation
73. Pretend to be someone else to gain access to information or services
74. Lack of secrecy
75. Eavesdrop on data over network
76. Corruption
77. Modify data over network
78. Break-ins
79. Take advantage of implementation bugs
80. Denial of Service
81. Flood resource to deny use from legitimate users
82. Firewalls
83. Filtering "dangerous: traffic at a middle point in the network
84. Network level security (e.g. IPsec)
85. Host-to-host encryption and authentication
86. Providing security without application knowledge
87. Application level security
88. True end-to-end security
89. Extra effort per application

90. Libraries help, like SSL/TLS

K. Hands-on and In-Class Activities

91. Labs
92. Workshops
93. Group Activities

L. Cryptography and Modern Cryptography Workshop

94. Working with Block ciphers
95. Case studies: AES and 3DES.
96. How to use block ciphers
97. Message integrity: definition and applications
98. Case studies: SHA and HMAC
99. Authenticated encryption: security against active attacks
100. Public key cryptography
101. Public key encryption
102. Digital signatures: definitions and applications
103. How to sign using RSA
104. Hash based signatures
105. Working with certificates, certificate transparency, certificate revocation
106. Authenticated key exchange and SSL/TLS session setup
107. Cryptography and quantum computers
108. Practical Constructions of Symmetric-Key Primitives, Public-Key (Asymmetric)
109. Cryptography, and end-to-end encryption
110. Message Authentication Codes (MAC) and hash functions and applications
111. Digital Signature Schemes
112. Protocols for identification and login

CLASS ROOM TRAINING – ONLINE AND OFFLINE

The training includes Single user Classroom / laboratory teaching, learning and simulation software module. The content has easy explanation of various complex topics with animation and simulation for ease of student learning. It also supports learning through videos, graphs, charts, along with mandatory rich content and theory to understand fundamental concepts, interactive learning objects, FAQ, MCQ etc. The content is supplied in digital online access or license protection.

Contact US

Registered Office

SIGMA TRAINERS AND KITS
E-113, Jai Ambe Nagar,
Near Udgam School,
Drive-in Road,
Thaltej,
AHMEDABAD-380054. INDIA.

Factory

SIGMA TRAINERS AND KITS
B-6, Hindola Complex,
Below Nishan Medical Store,
Lad Society Road,
Near Vastrapur Lake,
AHMEDABAD-380015. INDIA.

Contact Person

Prof. D R Luhar – Director

Mobile	: 9824001168
Whatsapp	: 9824001168

Phones:

Office	: +91-79-26852427
Factory	: +91-79-26767512
	+91-79-26767648
	+91-79-26767649

E-Mails :

sales@sigmatrainers.com
drluhar@gmail.com