CISSP

Key Areas of Knowledge -- Cryptography

Know	Basic concepts including: • Public and private key algorithms • Algorithm construction • Key distribution and management • Methods of attack • Public key cryptography
Understand	Application and use of cryptography and cryptographic systems for • Confidentiality • Integrity • Authenticity • Non-repudiation
Understand	Encryption methods including: • One time pads • Substitutions • Permutations
Understand	Encryption types including • Stream • Block as well as related terms including initialization vectors (IV)
Understand	Message digest/hashing including: • MD5 • SHA • HMAC
Utilize	Digital signatures to provide electronic transactions authenticity
Employ	Cryptography in network security (SSL, IPSEC)
Maintain	E-Mail security with PGP or S/MIME
Name	Cryptographic alternatives e. g. steganography and watermarking

Take from:
*CISSP -- Candidate Information Bulletin, downloaded 30 Jun*e 08