4.1 Knowledge Area: Data Security

The Data Security knowledge area focuses on the protection of data at rest, during processing, and in transit. This knowledge area requires the application of mathematical and analytical algorithms to fully implement.

4.1.1 Knowledge Units and Topics

The following table lists the essentials, knowledge units, and topics of the Data Security knowledge area.

DATA SECURITY

Essentials

- Basic cryptography concepts,
- Digital forensics,
- End-to-end secure communications,
- Data integrity and authentication, and
- Information storage security.

Knowledge Units	**Topics**	**Description/Curricular Guidance**
Cryptography		
	Basic concepts	This topic covers basic concepts in cryptography to build the base for other sections in the knowledge unit. This topic includes: ● Encryption/decryption, sender authentication, data integrity, non-repudiation, ● Attack classification (ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext), ● Secret key (symmetric), cryptography and public-key (asymmetric) cryptography, ● Information-theoretic security (one-time pad, Shannon Theorem), and ● Computational security.
	Advanced concepts	This topic includes: ● Advanced protocols: o Zero-knowledge proofs, and protocols, o Secret sharing, o Commitment, o Oblivious transfer, o Secure multiparty computation, ● Advanced recent developments: fully homomorphic encryption, obfuscation, quantum cryptography, and KLJN scheme.

	Mathematical background	This topic is essential in understanding encryption algorithms. More advanced concepts may be included, if needed. This topic includes: ● Modular arithmetic, ● Fermat, Euler theorems, ● Primitive roots, discrete log problem, ● Primality testing, factoring large integers, ● Elliptic curves, lattices and hard lattice problems, ● Abstract algebra, finite fields, and ● Information theory.
	Historical ciphers	This topic includes the following and their current applications (if any): ● Shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, and ● Hill cipher, Enigma machine, and others.
	Symmetric (private key) ciphers	This topic includes: ● B block ciphers and stream ciphers (pseudo-random permutations, pseudo-random generators), ● Feistel networks, Data Encryption Standard (DES), ● Advanced Encryption Standard (AES), ● Modes of operation for block ciphers, ● Differential attack, linear attack, and ● Stream ciphers, linear feedback shift registers, RC4.
	Asymmetric (public-key) ciphers	This topic includes: ● Theoretical concepts (Computational complexity, one-way trapdoor functions), ● Naive RSA, ● Weakness of Naive RSA, padded RSA, ● Diffie-Hellman protocol, ● El Gamal cipher, ● Other public-key ciphers, including Goldwasser-Micali, Rabin, Paillier, McEliece, and ● Elliptic curves ciphers.
Digital Forensics [*See also System Security KA for related content,*]		
	Introduction	This topic includes: ● Definition, and ● Limits and types of tools (open source versus closed source).

	Legal Issues	This topic includes: ● Right to privacy, ● Fourth and Fifth Amendments, ● Protection of encryption keys under the Fifth Amendment, ● Types of legal authority (owner consent, search warrant, FISA, Title III (wiretap), abandonment, exigent circumstances, plain sight, etc.), ● Protection from legal processes (e.g., ISP subscriber information via subpoena, e-mail server transactional data from 2703(d) court order, full content via search warrant, etc.), ● Legal request for preservation of digital evidence (e.g., via 2703(f) preservation letter), and ● Affidavits, testimony and testifying,
	Digital forensic tools	This topic includes: ● Types, ● Artifact-focused versus all-in-one tools, ● Requirements, and ● Limitations.
	Investigatory process	This topic includes: ● Alerts, ● Identification of evidence, ● Collection and preservation of evidence, ● Timelines, reporting, chain of custody, and ● Authentication of evidence.
	Acquisition and preservation of evidence	This topic includes: ● Pull-the-plug versus triage, ● Write-blocking, ● Forensically-prepared destination media, ● Imaging procedures, ● Acquisition of volatile evidence, ● Live forensics analysis, and ● Chain of custody.
	Analysis of evidence	This topic focuses on knowledge (awareness the artifact exists), attributes (components and possible variations of the artifact), origin/cause (emphasis on why the artifact exists), discoverability (how the artifact is located/viewed with tools), relevance (significance in the context of the specific investigation). This includes: ● Sources of digital evidence, ● Deleted and undeleted files, temporary files, ● Metadata, ● Print spool files, ● Slack space, ● Hibernation files, ● Windows registry, ● Browser history, ● Log files, ● File systems, ● File recovery, and ● File carving.

	Presentation of results	This topic includes: ● Timeline analysis, ● Attribution, ● Lay versus technical explanations, ● Executive summaries, ● Detailed reports, and ● Limitations.
	Authentication of evidence	This topic includes: ● Hashing algorithms (MD5, SHA-1, etc.), ● Hashing entire media vs individual files, and ● Pre-exam and post-exam verification hashing.
	Reporting, incident response and handling	This topic includes: ● Report structures, ● Incident detection and analysis, ● Containment, eradication and recovery, ● Post-incident activities, and ● Information sharing,
	Mobile forensics	This topic includes: ● Wireless technologies, ● Mobile device technology, ● Collection/Isolation of mobile device, ● Mobile operating systems (OS) and Apps, and ● Mobile artifacts.
Data Integrity and Authentication		
	Authentication strength	This topic includes: ● Multifactor authentication, ● Cryptographic tokens, ● Cryptographic devices, ● Biometric authentication, ● One-time passwords, and ● Knowledge-based authentication.
	Password attack techniques	This topic includes: ● Dictionary attack, ● Brute force attack, ● Rainbow table attack, ● Phishing and social engineering, ● Malware-based attack, ● Spidering, ● Off-line analysis, and ● Password cracking tools.
	Password storage techniques	This topic includes: ● Cryptographic hash functions (SHA-256, SHA-3, collision resistance), ● Salting, ● Iteration count, and ● Password-based key derivation.

	Data integrity	This topic includes: ● Message authentication codes (HMAC, CBC-MAC), ● Digital signatures, ● Authenticated encryption, and ● Hash trees.
Access Control		
	Physical data security	This topic includes: ● Data center security, including keyed access, man trips, key cards and video surveillance, ● Rack-level security, and ● Data destruction.
	Logical data access control	This topic includes: ● Access control lists, group policies, passwords, ● Discretionary Access Control (DAC), ● Mandatory Access Control (MAC), ● Role-based Access Control (RBAC), ● Attribute-based Access Control (ABAC), ● Rule-based Access Control (RAC), ● History-based Access Control (HBAC), ● Identity-based Access Control (IBAC), ● Organization-based Access Control (OrBAC), and ● Federated identities and access control.
	Secure architecture design	This topic includes: ● Principles of a security architecture, and ● Protection of information in computer systems.
	Data leak prevention techniques	This topic includes: ● Controlling authorized boundaries, ● Channels, ● Destinations, and ● Methods of data sharing.
Secure Communication Protocols		
	Application and transport layer protocols	This topic includes: ● HTTP, ● HTTPS, ● SSH, and ● SSL/TLS.
	Attacks on TLS	This topic includes: ● Downgrade attacks, ● Certificate forgery, ● Implications of stolen root certificates, and ● Certificate transparency.
	Internet/Network layer	This topic includes IPsec and VPN.
	Privacy preserving protocols	This topic includes Mixnet, Tor, Off-the-record message, and Signal.
	Data link layer	This topic includes L2TP, PPP and RADIUS.

Cryptanalysis		
	Classical attacks	This topic includes: ● Brute-force attack, ● Frequency-based attacks, ● Attacks on the Enigma machine, and ● Birthday-paradox attack.
	Side-channel attacks	This topic includes: ● Timing attacks, ● Power-consumption attacks, and ● Differential fault analysis.
	Attacks against private-key ciphers	This topic includes: ● Differential attack, ● Linear attack, and ● Meet-in-the-middle attack.
	Attacks against public-key ciphers	This topic includes factoring algorithms (Pollard's p-1 and rho methods, quadratic sieve, and number field sieve).
	Algorithms for solving the Discrete Log Problem	This topic includes: ● Pohlig-Hellman, ● Baby Step/Giant Step, and ● Pollard's rho method.
	Attacks on RSA	This topic includes: ● Shared modulus, ● Small public exponent, and ● Partially exposed prime factors.
Data Privacy [*See also Human Security KA, Organizational Security KA, and Societal Security KA for related content.*]		
	Overview	This topic includes: ● Definitions (Brandeis, Solove), ● Legal (HIPAA, FERPA, GLBA), ● Data collection, ● Data aggregation, ● Data dissemination, ● Privacy invasions, ● Social engineering, and ● Social media.
Information Storage Security		
	Disk and file encryption	This topic includes hardware-level versus software encryption.

	Data erasure	This topic includes: ● Overwriting, degaussing, ● Physical destruction methods, and ● Memory remanence.
	Data masking	For this topic, include the need and techniques for data masking. The following is a non-exhaustive list of subtopics to be covered: ● Data masking for testing, ● Data masking for obfuscation, and ● Data masking for privacy.
	Database security	This topic includes: ● Access/authentication, auditing, and ● App integration paradigms.
	Data security law	This topic introduces the legal aspects of data security, laws and policies that govern data (e.g., HIPAA). It also provides an introduction to other law-related topics in the Organizational Security knowledge area.

4.1.2 Essentials and Learning Outcomes

Students are required to demonstrate proficiency in each of the essential concepts through achievement of the learning outcomes. Typically, the learning outcomes lie within the *understanding* and *applying* levels in the Bloom's Revised Taxonomy (http://ccecc.acm.org/assessment/blooms).

Essentials	Learning outcomes
Basic cryptography concepts	
	Describe the purpose of cryptography and list ways it is used in data communications.
	Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext in ciphertext.
	Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities.
	Discuss the dangers of inventing one's own cryptographic methods.
	Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
End-to-end secure communications [*See also Connection Security KA for related content*]	
	Explain the goals of end-to-end data security.
Digital forensics	
	Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics.
	Compare and contrast variety of forensics tools.

Data integrity and authentication	
	Explain the concepts of authentication, authorization, access control, and data integrity.
	Explain the various authentication techniques and their strengths and weaknesses.
	Explain the various possible attacks on passwords.
Data erasure	Describe the various techniques for data erasure.