Subject:	Computer Science	**Course/Grade Level:**	Computer Security / 11th-12th
Focus Statement:	Students will demonstrate how cryptography works and show how to secure web applications.		

Outcome 1:

CTE.CS.1		**Students will show how cryptography is used to encrypt information.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.1.1	Describe the main components of symmetric cryptography.
NA	NA	CTE.CS.1.2	Explain the difference between cryptanalysis and brute-force attacks.
NA	NA	CTE.CS.1.3	Understand the operation of a monoalphabetic substitution cipher.
NA	NA	CTE.CS.1.4	Understand the operation of a polyalphabetic substitution ciper.
NA	NA	CTE.CS.1.5	Describe how a rotor machine can be used to encrypt a message.

Outcome 2:

CTE.CS.2		**Students will show how modern block ciphers function.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.2.1	Explain the difference between stream ciphers and block ciphers.
NA	NA	CTE.CS.2.2	Explain the structure of the Festal cipher.
NA	NA	CTE.CS.2.3	Explain how encryption is the inverse of decryption.
NA	NA	CTE.CS.2.4	Explain how the Data Encryption Standard (DES) works.
NA	NA	CTE.CS.2.5	Explain the avalanche effect.
NA	NA	CTE.CS.2.6	Explain how the Advanced Encryption Standard (AES) differs from the DES.
NA	NA	CTE.CS.2.7	Understand the four transformations used in the Advanced Encryption Standard (AES).
NA	NA	CTE.CS.2.8	Explain the AES key expansion algorithm.
NA	NA	CTE.CS.2.9	Analyze the security of multiple encryption schemes.
NA	NA	CTE.CS.2.10	Explain how a meet-in-the-middle attack works.

NA	NA	CTE.CS.2.11	Compare and contrast ECB, CBC, CFB, OFB, and counter modes of operation.
NA	NA	CTE.CS.2.12	Explain the XTS-AES mode of operation.

Outcome 3:

CTE.CS.3		**Students will show how random and pseudorandom number generation works.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.3.1	Understand the differences among true random number generators, pseudorandom number generators, and pseudorandom functions.
NA	NA	CTE.CS.3.2	Describe the requirements for a pseudorandom number generator.
NA	NA	CTE.CS.3.3	Explain how a block cipher can be used to construct a pseudorandom number generator.
NA	NA	CTE.CS.3.4	Explain how the RC4 stream cipher works.
NA	NA	CTE.CS.3.5	List some possible sources of true random numbers.
NA	NA	CTE.CS.3.6	Explain the purpose of deskewing a true random number generator.

Outcome 4:

CTE.CS.4		**Students will show how public-key cryptosystems work.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.4.1	Explain how a public-key cryptosystem works.
NA	NA	CTE.CS.4.2	Describe multiple uses of a public-key cryptosystem.
NA	NA	CTE.CS.4.3	Explain the requirements of a public-key cryptosystem.
NA	NA	CTE.CS.4.4	Explain how the RSA algorithm works.
NA	NA	CTE.CS.4.5	Explain how a timing attack works.

Outcome 5:

CTE.CS.5		**Students will utilize cryptographic hash functions.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.5.1	List some applications of cryptographic hash functions.
NA	NA	CTE.CS.5.2	Explain why a has function used for message authentication must be secured.

NA	NA	CTE.CS.5.3	Explain the differences among preimage resistant, second preimage resistant, and collision resistant properties.
NA	NA	CTE.CS.5.4	Explain how a cryptographic hash function works.
NA	NA	CTE.CS.5.5	Explain how the Secure Hash Algorithm (SHA) works.
NA	NA	CTE.CS.5.6	Explain the birthday paradox.

Outcome 6:

CTE.CS.6		**Students will implement a message authentication code.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.6.1	List some possible attacks related to message authentication.
NA	NA	CTE.CS.6.2	Explain a message authentication code.
NA	NA	CTE.CS.6.3	Describe the keyed-hash message authentication code (HMAC) algorithm.
NA	NA	CTE.CS.6.4	Describe the cypher-based message authentication code (CMAC) algorithm.
NA	NA	CTE.CS.6.6	Explain the CCM and GCM modes of operation.

NA	NA	CTE.CS.6.7	Use a hash function or message authentication code for pseudorandom number generation.

Outcome 7:

CTE.CS.7		**Students will secure a web application.**	
Pacing:		**Local Code:**	**Components:**
Instruct	**Assess**		**Students will:**
NA	NA	CTE.CS.7.1	Implement a SQL injection on a practice website.
NA	NA	CTE.CS.7.2	Secure a website against SQL injections.
NA	NA	CTE.CS.7.3	Explain how an upload attack vector can compromise the security of a web application.
NA	NA	CTE.CS.7.4	Implement a cross site scripting (XSS) attack on a practice website.
NA	NA	CTE.CS.7.5	Secure a website against XSS attacks.
NA	NA	CTE.CS.7.6	Securely encode sensitive data on a web application.