Goals and Learning Objectives

The learning objective for this section is to understand the fundamentals of encryption, symmetric, asymmetric, hashers, SSL, TLS, certificates, SSL stripping, and the weaknesses inherent in encryption.

Symmetric Encryption

Encryption is a method of transforming readable data, called plain text, into a form that is unreadable, which is called cipher text. This enables the storage or transmission of data in a form that is unreadable and which remains confidential and private.

Decryption is a method to transform cipher text back into readable plain text.

To simplify things, there are two main components of encryption that you can think about. There is the algorithm, and there is the key.

AES, symmetric encryption algorithm, uses just one key

The password is converted to the key using something called a key derivation function.

you can see 128-bit, and you can see 256-bit. 256-is the bit length, or you can consider it the strength of the algorithm.

AES *= Symmetric Algorithms (Uses 1 key)*
Password becomes the Key
e.g. password123 > zcEXvO!XMITczI8!G%u0

Symmetric Encryption Algorithms:
• Data Encryption Standard (DES)
• Triple-DES (3DES)
• Blowfish
• RC4
• RC5
• RC6
• Advanced Encryption Standard (AES)

Asymmetric Encryption

Asymmetric = 2 Keys (Public and Private)
Symmetric = 1 Key (Private)

public and private are the two keys that are used in asymmetric encryption. So we have symmetric encryption = one key, asymmetric encryption = two keys, the public and private key