Symmetric encryption

Now that you understand random permutations and how they are simulated in cryptography, this module will show you how they are used to encrypt arbitrary length data. We will investigate the most used permutation, a "block cipher" called AES. We will also see how to use a popular cryptographic toolkit to encrypt using these methods.

Learning objectives

By the end of this module you should be able to...

- Encrypt and decrypt data using a permutation and various modes-of-operation (eg, ECB, CBC, CTR);
- Explain the security model used for the modes;
- Simulate each of the stages of an AES round;
- Compute by hand operations in the field GF(2^n); and
- Use a cryptographic toolkit to encrypt and decrypt data.