X.800 security architecture categories: confidentiality, data integrity, authentication, non-repudiation, access control

23 mod 5 = 3

MAC does not provide a digital signature because both sender and receiver share the same key.

Where H(X) = 32, when we learn (X mod 7), we reduce the entropy by 2.83 bits.

-(0.33\*log2(0.33) + 0.33\*log2(0.33) + 0.34\*log2(0.34))

Self-synchronizing stream ciphers have a key generated independently of ciphertext

In Double DES, plaintext is encrypted twice with 2 different keys.

Variant Beaufort cipher is the inverse of the Vigenere cipher.

Running key ciphers do not acquire perfect secrecy even if the key is as long as the message.

We can swap byte substitution & shift rows, and mix columns & add round key in Rijndael.

Add Round Key does not provide diffusion and confusion.

Virtually all cryptographic hash functions involve iterative use of a compression function.

Encryption hardware is optimised toward larger data sizes

where d1, d