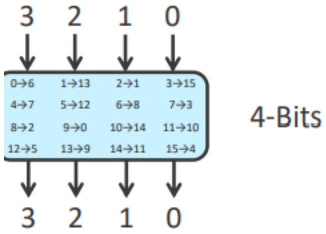
Contents

1 Block Ciphers

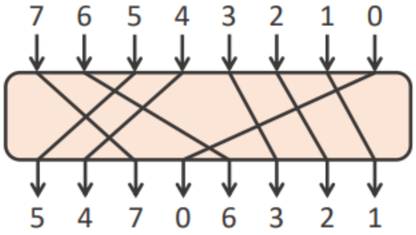
- Block ciphers use a key to encrypt a fixed-size block of plaintext into a fixed-size block of ciphertext
- If youre careful, you can convert between block and stream ciphers using modes of operation

2 SP-Networks

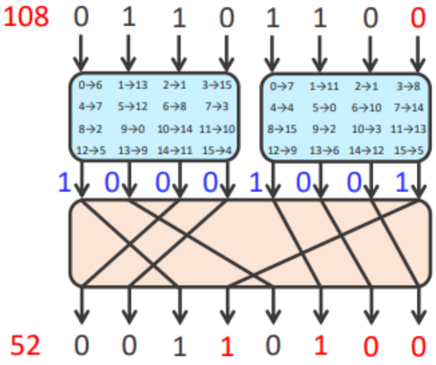
- Claude Shannon suggested that all that was required for a strong cipher was repeated **substitution and permutation**
- SP-Networks combine a substitution process with a permutation into a single round
- Rounds are then repeated enough times to ensure the algorithm is secure
- **Substitution Boxes** Add confusion by replacing values with other values using a lookup table



- **Permutation Boxes** Add diffusion by moving values around from input to output



- Combined, result in:

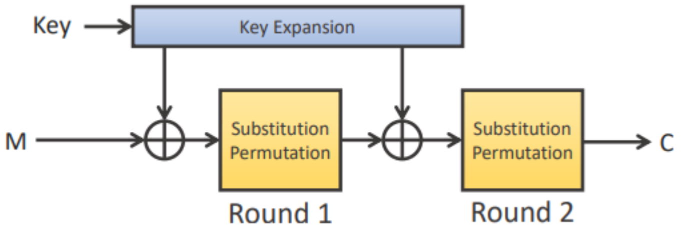


2.1 Notes

- One Round **isnt enough**!
- Careful analysis of input changes and output changes can reveal the contents of the S-boxes
- More rounds produces more diffusion
- Replacing permutation with linear transformation is more effective. Each bit is the XOR combination of multiple S-box outputs
- Typically the box size is around 128-bit and 256-bit.
- ”Psuedorandomness” of the result is compromised with poor S-box design

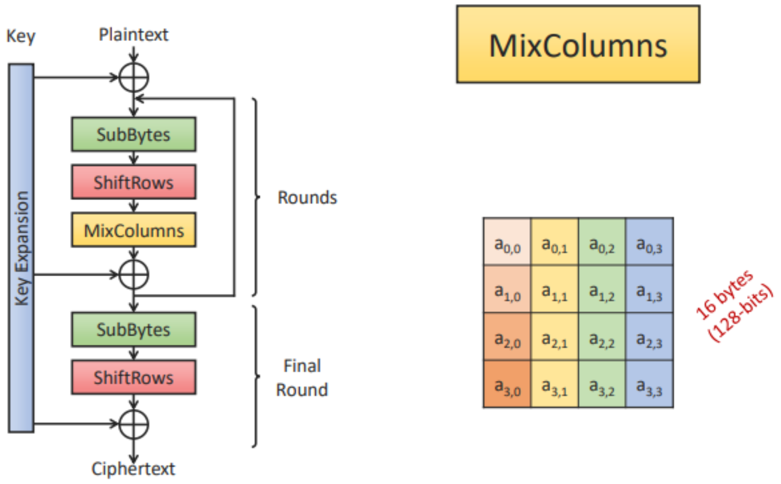
2.2 Key Mixing

The previous SP-network didnt use a key, we can add one using XOR:



3 Advanced Encryption Standard

- Superseded DES as a standard in 2002. A standard built around the Rijndael algorithm
- Rijndael is an SP-Network with a 128-bit block size, and a key length of 128, 192 or 256-bits
- Round count depends on key length. 10, 12 or 14 cycles
- AES is vastly superior to DES, which had a 64-bit block and 56 bit key
- AES uses rounds of 4 layers, and a final round of 3. Bytes are represented as a 4x4 block called the state



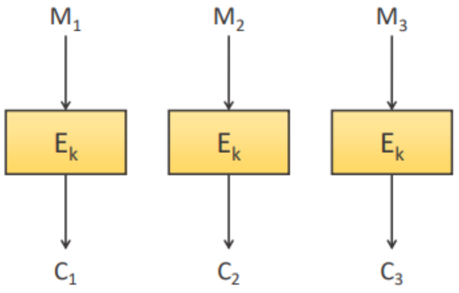
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

4 Block Cipher Modes

- Most messages dont come in convenient 128-block lengths
- Well need to run a block cipher repeatedly on consecutive blocks

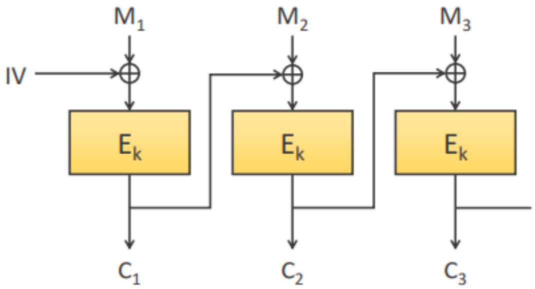
4.1 Electronic Code Book (ECB)

- Just encrypt each block one after another
- Weak to redundant data divulging patterns



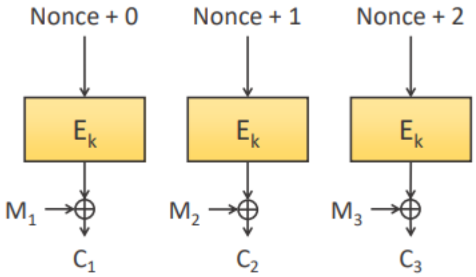
4.2 Cipher Block Chaining (CBC)

- XOR the output of each cipher block with the next input
- Not totally immune to the insertion of malicious blocks



4.3 Counter Mode (CTR)

- Encrypting a counter
- Can be parallelized! 22 to produce a stream cipher



Reference section

placeholder