Block Ciphers

Dr Rosanne English

Blocks Example

```
10110101110010101011101010
```

```
1011 0101 1100 1010 1110 1010
```

A Basic Block Cipher

For each block:

1. Split in two
2. Switch halves
3. Do XOR with key

`01100010 01111001 01100101 01100010 01101111 01100010` plaintext

`01101101` key

`01001011 11111010` ciphertext

Padding

Cryptographic Message Syntax (CMS) from RFC 8933

Pad at trailing end with k-(l mod k) octets with all with the value k-(l mod k)

E.g. key of 8 bytes, message of 12 bytes has 4 padding bytes of value 4

Caveat: This form of padding with a short message can potentially lead to a Bleichenbacher attack