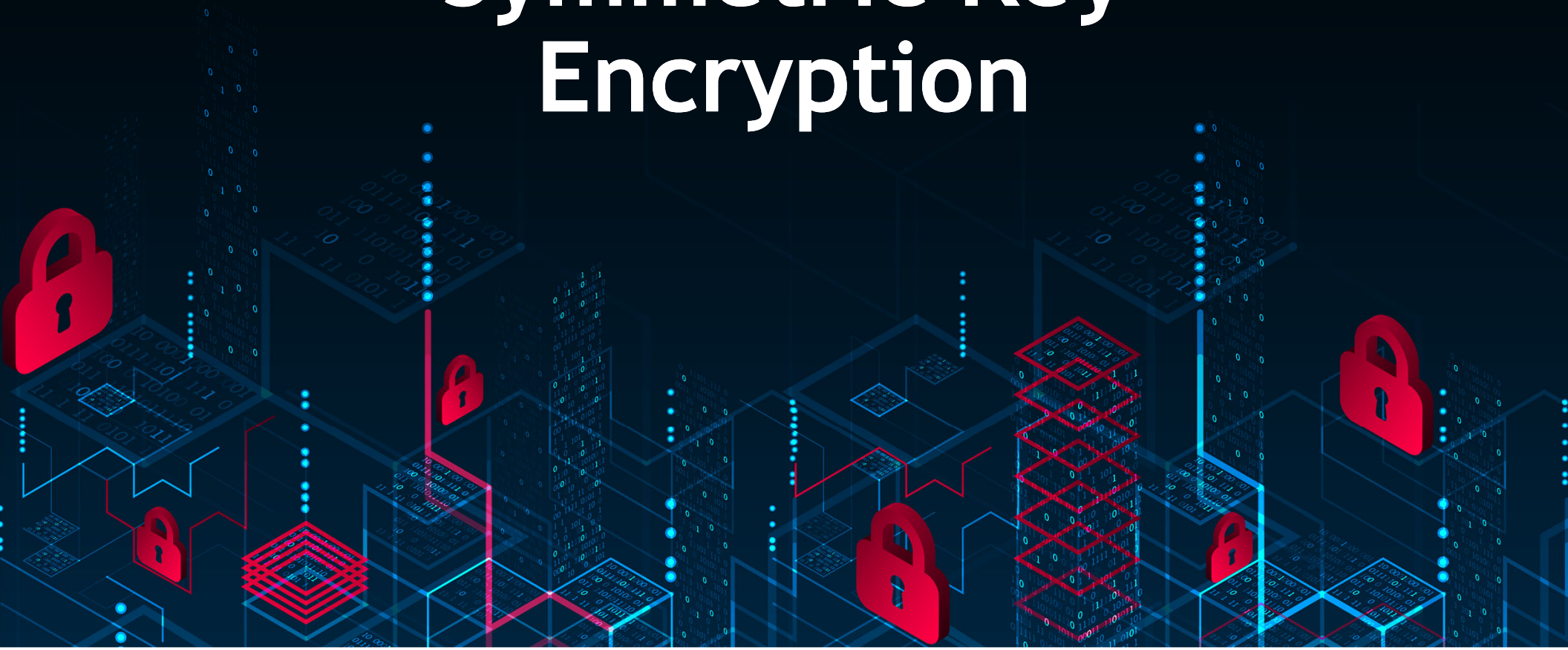
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Symmetric Key Encryption



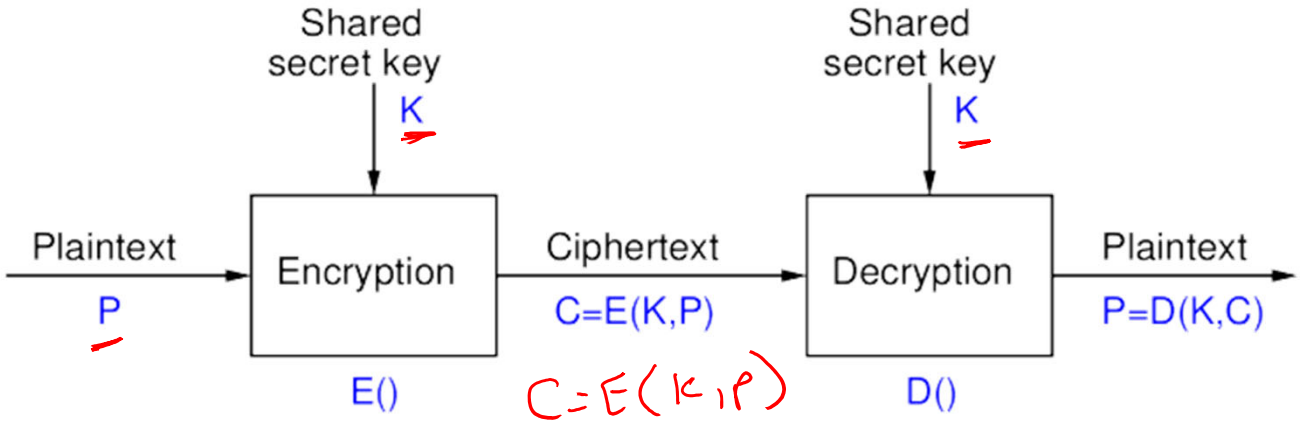
Video Summary

- What is symmetric key encryption
- Assumptions
- Symmetric key encryption algorithms (DES, 3DES, AES)
- Encryption For Confidentiality
- Attacks on Encryption Algorithms

Symmetric Key Encryption for Confidentiality

- Symmetric key encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information.
- The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.
- Some examples of where symmetric cryptography is used are:
  - ✓ Payment applications, such as CC transactions to prevent identity theft or fraudulent charges
  - ✓ Validations to confirm that the sender of a message is who he claims to be
  - ✓ Hashing or Random number generation

Symmetric Key Encryption for Confidentiality



Requirements

- Strong encryption algorithm: given algorithm, ciphertext and known pairs of (plaintext, ciphertext), attacker should be unable to find plaintext or key
- Shared secret keys: sender and receiver both have shared a secret key; no-one else knows the key

Assumptions: Symmetric Key Encryption

- The same secret key, K, is used for encryption, E(), and decryption, D(). The secret is shared between two entities, i.e. K_{AB}.
- Encrypting plaintext, P, with a key, produces ciphertext C, e.g. $C = \mathrm{E}(K_{AB}, P)$.
- Decrypting ciphertext with the correct key will produce the original plaintext. The decrypter will be able to recognise that the plaintext is correct (and therefore the key is correct). E.g. $P = \mathrm{D}(K_{AB}, C)$.
- Decrypting ciphertext using the incorrect key will *not* produce the original plaintext. The decrypter will be able to recognise that the key is wrong, i.e. the decryption will produce unrecognisable output.

Data Encryption Standard (DES)

- Designed by IBM and NSA; standardised by NIST in 1977 as FIPS-46
  - 1999: NIST recommended Triple-DES; DES only for legacy systems
  - 2005: FIPS-46 standard withdrawn
- Block size: 64 bits
- Key length: 56 bits (64 bits, but 8 are parity)
- Initial and final permutations, then 16 rounds, each involving permutations and substitutions
- Decryption is almost identical to encryption → single implementation for both algorithms
- Key size is insecure; algorithm considered secure

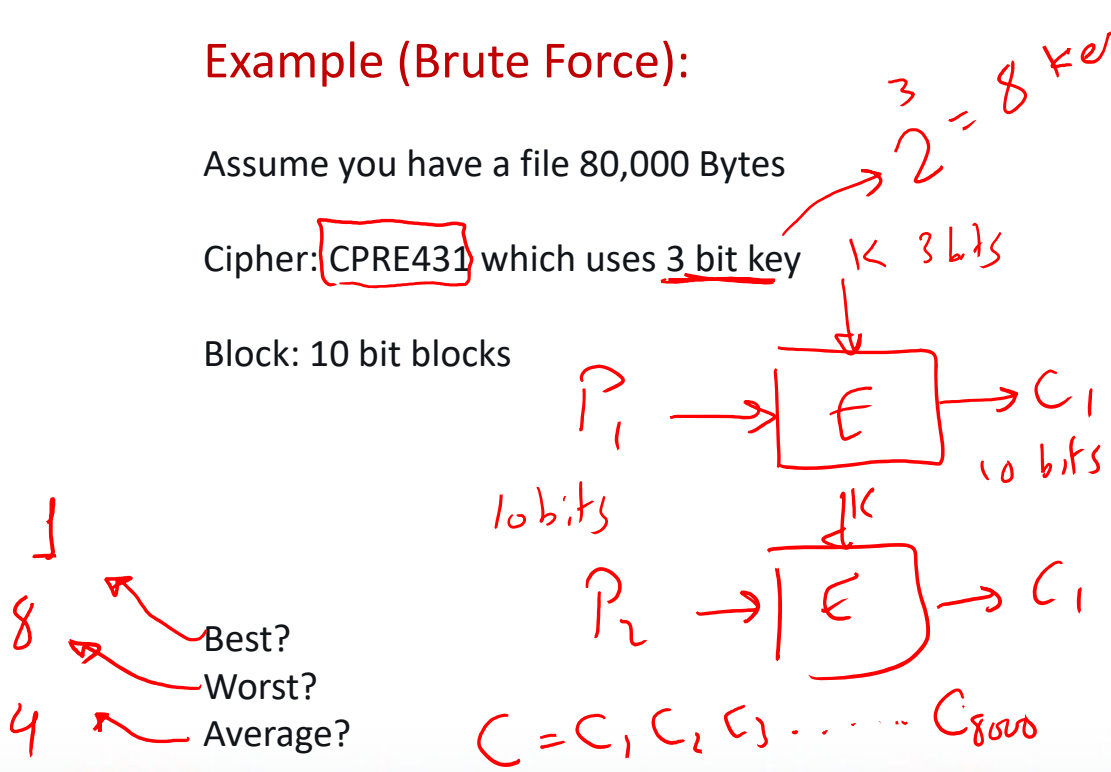
Data Encryption Standard (DES)

Example (Brute Force):

Assume you have a file 80,000 Bytes

Cipher: CPRE431 which uses 3 bit key

Block: 10 bit blocks



Data Encryption Standard (DES)

Example (Brute Force):

Assume you have a file 80,000 Bytes

Cipher: DES which uses 56 bit key

Block: 10 bit blocks

56 bit key

2^{56} keys $= 7.2 \times 10^{16}$ key

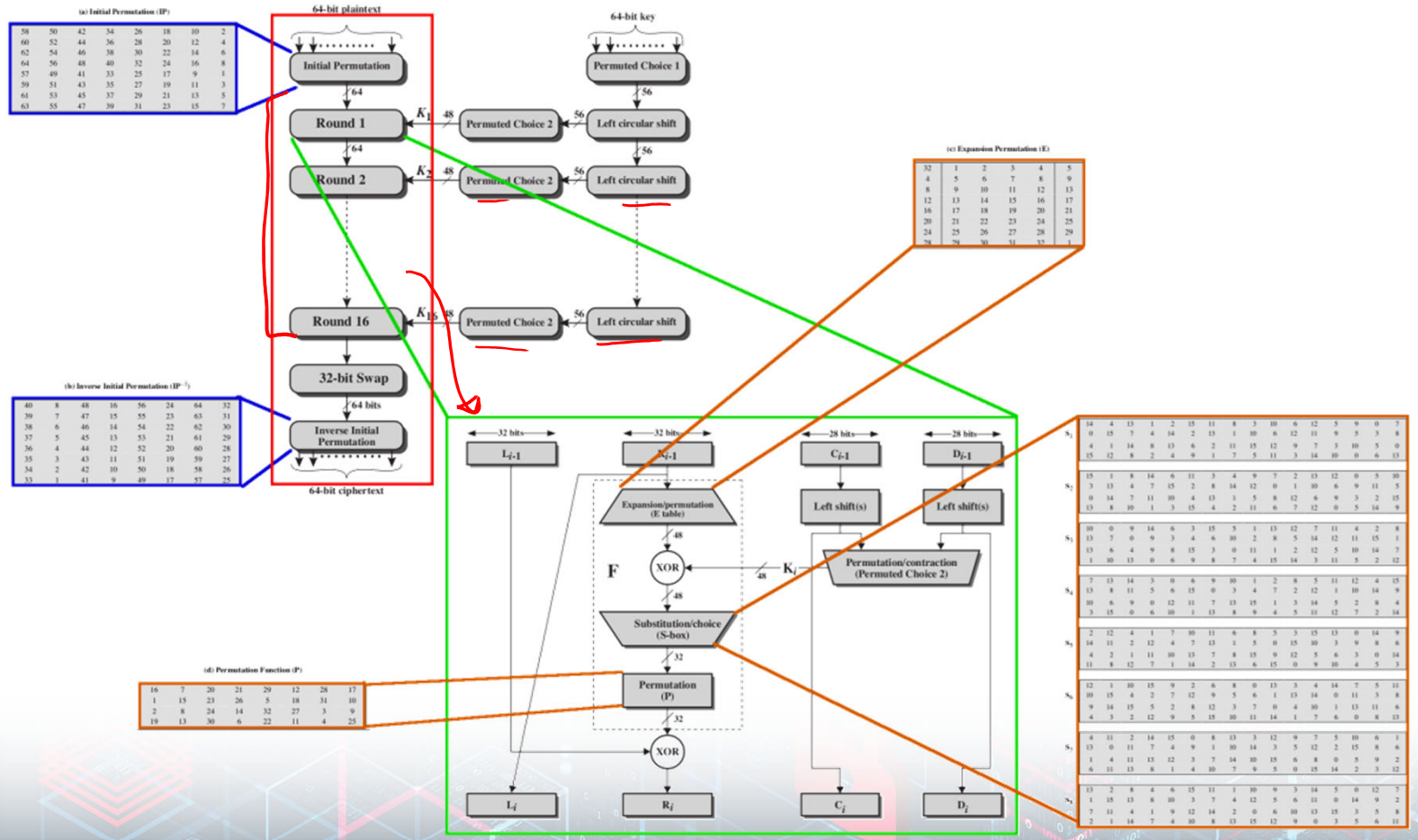
Best? 1

Worst? 2^{56}

Average? $2^{55} = \frac{2^{56}}{2}$

Note that DES uses 56 keys

Data Encryption Standard (DES)



Data Encryption Standard (DES)

```
$ xxd -b -c 8 msg1.txt
0000000: 01001000 01100101 01101100 01101100 01101111 00101110 00100000 01010100  Hello. T
0000008: 01101000 01101001 01110011 00100000 01101001 01110011 00100000 01101111  his is o
0000010: 01110101 01110010 00100000 01110011 01110101 01110000 01100101 01110010  ur super
0000018: 00100000 01110011 01100101 01100011 01110010 01100101 01110100 00100000   secret
0000020: 01101101 01100101 01110011 01110011 01100001 01100111 01100101 00101110  message.
0000028: 00100000 01001011 01100101 01100101 01110000 00100000 01101001 01110100   Keep it
0000030: 00100000 01110011 01100101 01100011 01110010 01100101 01110100 00100000   secret
0000038: 01110000 01101100 01100101 01100001 01110011 01100101 00101110 00100000  please.
0000040: 01000111 01101111 01101111 01100100 01100010 01111001 01100101 00101110  Goodbye.
$ xxd -b -c 8 ciphertext.txt
0000000: 10000110 10010101 01101110 10100010 11001101 10101100 00010111 01100101  ..n....e
0000008: 11110101 01110011 01100110 10000110 11011000 11001100 10110101 01110111  .sf....w
0000010: 10111111 10011101 10011101 01111000 10100001 00100000 10000110 01101100  ...x. .l
0000018: 01101010 11101010 00111000 01101101 00011010 10101100 10110111 01000011  j.8m...C
0000020: 10100100 00011111 00100110 11000010 01001100 01011100 10010010 11000101  ..&.L\..
0000028: 01000110 00010101 11101101 11100001 11010110 11010111 10111001 10001110  F.......
0000030: 01101010 11101010 00111000 01101101 00011010 10101100 10110111 01000011  j.8m...C
0000038: 11100111 11000111 10011111 00011100 10110000 01000001 01011110 10010001  .....A^.
0000040: 01111111 00010000 00000111 01010001 11110110 10101010 00010111 11000001  ...Q....
$
```

P

C

Video Summary

- What is symmetric key encryption
- Assumptions
- Symmetric key encryption algorithms (DES, 3DES, AES)
- Encryption For Confidentiality
- Attacks on Encryption Algorithms