SYMMETRIC KEY CRYPTOGRAPHY
Lecture 4b

COMPSCI 726
Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

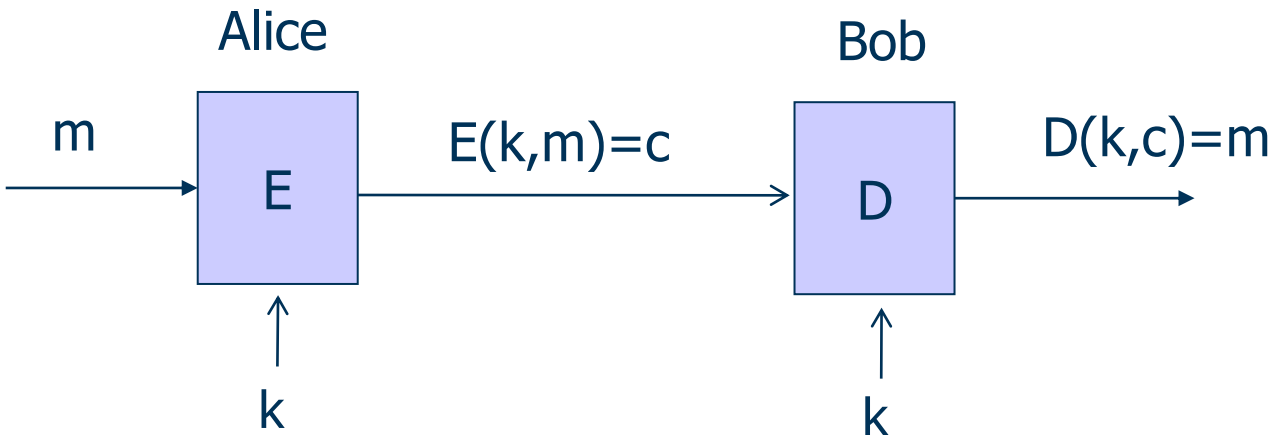
July 26, 2021

Source of most slides: **University of Twente**

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

SYMMETRIC ENCRYPTION

- Assumes parties already share a secret key (k)



- Encryption (E) and Decryption (D) algorithms are ***publicly known***
- m is a private message and c is ciphertext

HISTORY

- Monoalphabetic substitution
  - Caesar
- Polyalphabetic substitution
  - Vigenere
- Transposition cipher

CESAR CIPHER

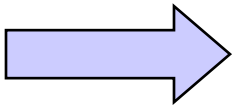
- Replace plaintext letter by letter 3 places further down the alphabet

Plaintext Letter	A	B	C	D	E	F	G	H	…
Ciphertext Letter	D	E	F	G	H	I	J	K	…

A=1, B=2, C=3, …

Encrypt: c = m+3
Decrypt: m = c-3

CESAR: EXAMPLE

“attackatdawn”  “dwwdfndwgdzq”

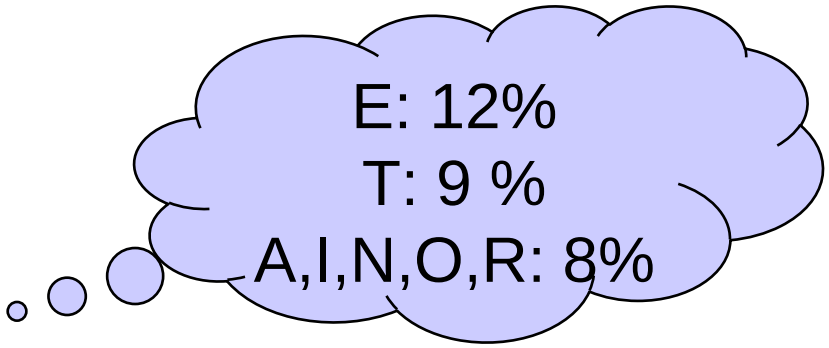
- Problem:
  - Letter frequency undisturbed
    - High frequency ciphertext letters map to high frequency plaintext letters
- Solution
  - Increase the blocksize
    - To at least 4-5 letters

VIGNERE CIPHER

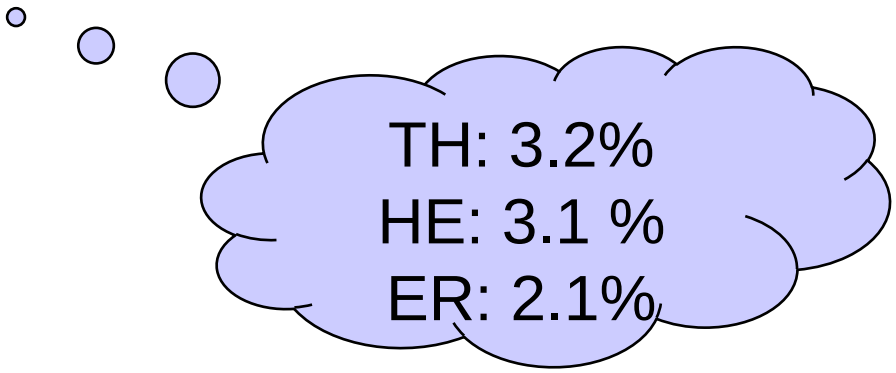
- Code letters as numbers (A=0, B=1, etc.)
- Key is basically a keyword
- Encrypt
  - Add keyword to plaintext (letter by letter)
- Decrypt
  - Subtract keyword from ciphertext
- Example

```
  WEAREDISCOVEREDSAVEYOURSELF
+ DECEPTIVEDECEPTIVEDECEPTIVE
------------------------------
  ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

ISSUES WITH VIGNERE CIPHER



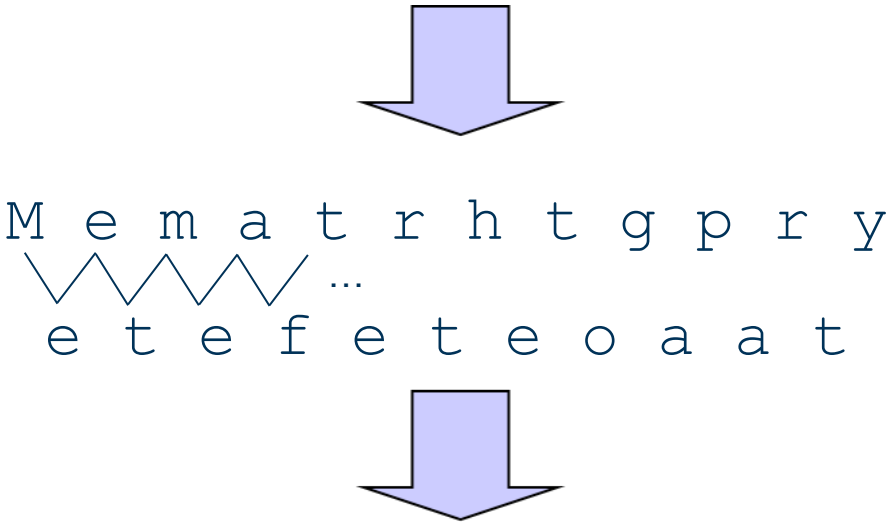
- Distribution of characters known
- Distribution of bigrams also known



TRANSPOSITION CIPHER

- Change order of letters in the message

“meet me after the toga party”



“mematrhtgpryetefeteoaat”

- Easy to detect: frequency distribution unchanged

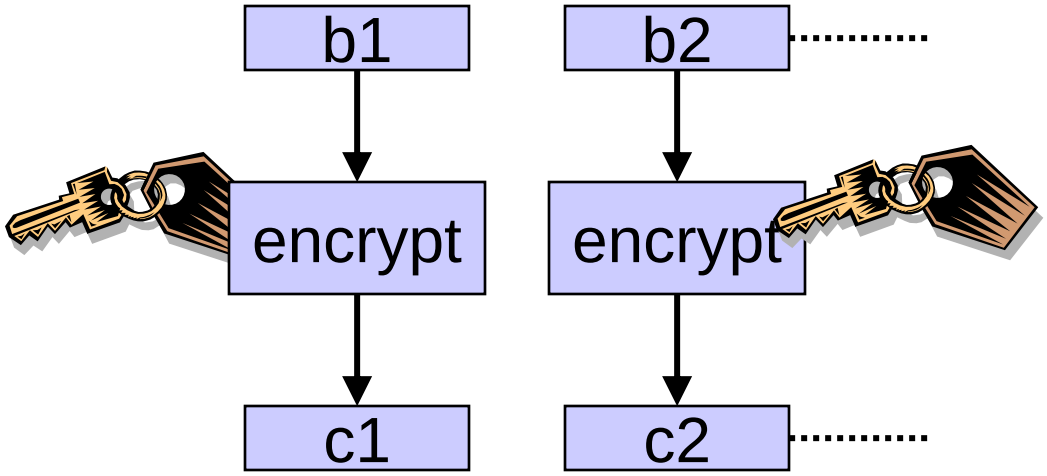
MODERN CIPHERS: PRINCIPLES

- Confusion
  - Substitution
- Diffusion
  - Transposition
- Commonly used symmetric key algorithms
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

ENCRYPTING LARGE MESSAGES

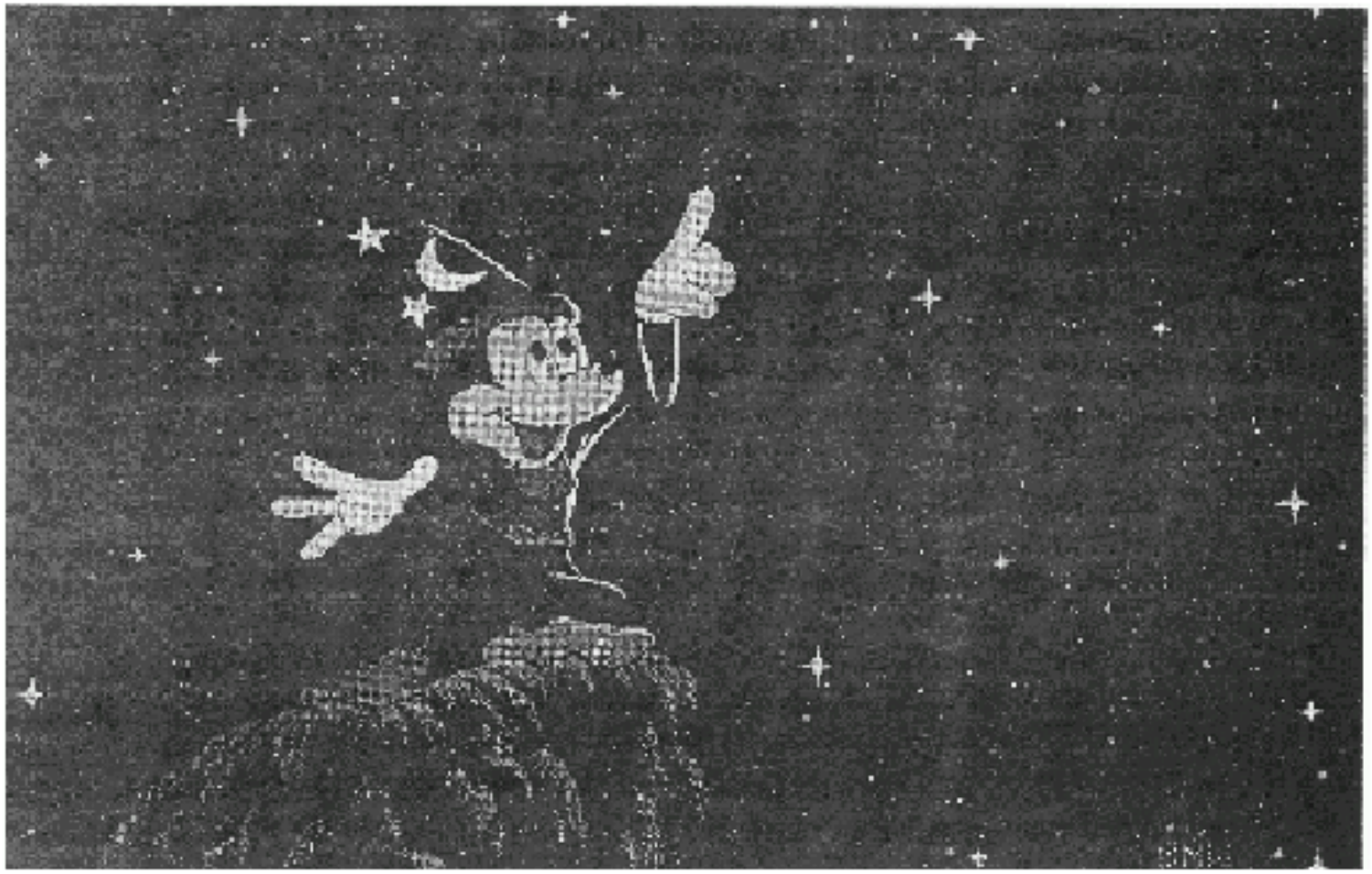
- Mode of operation
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

ECB MODE



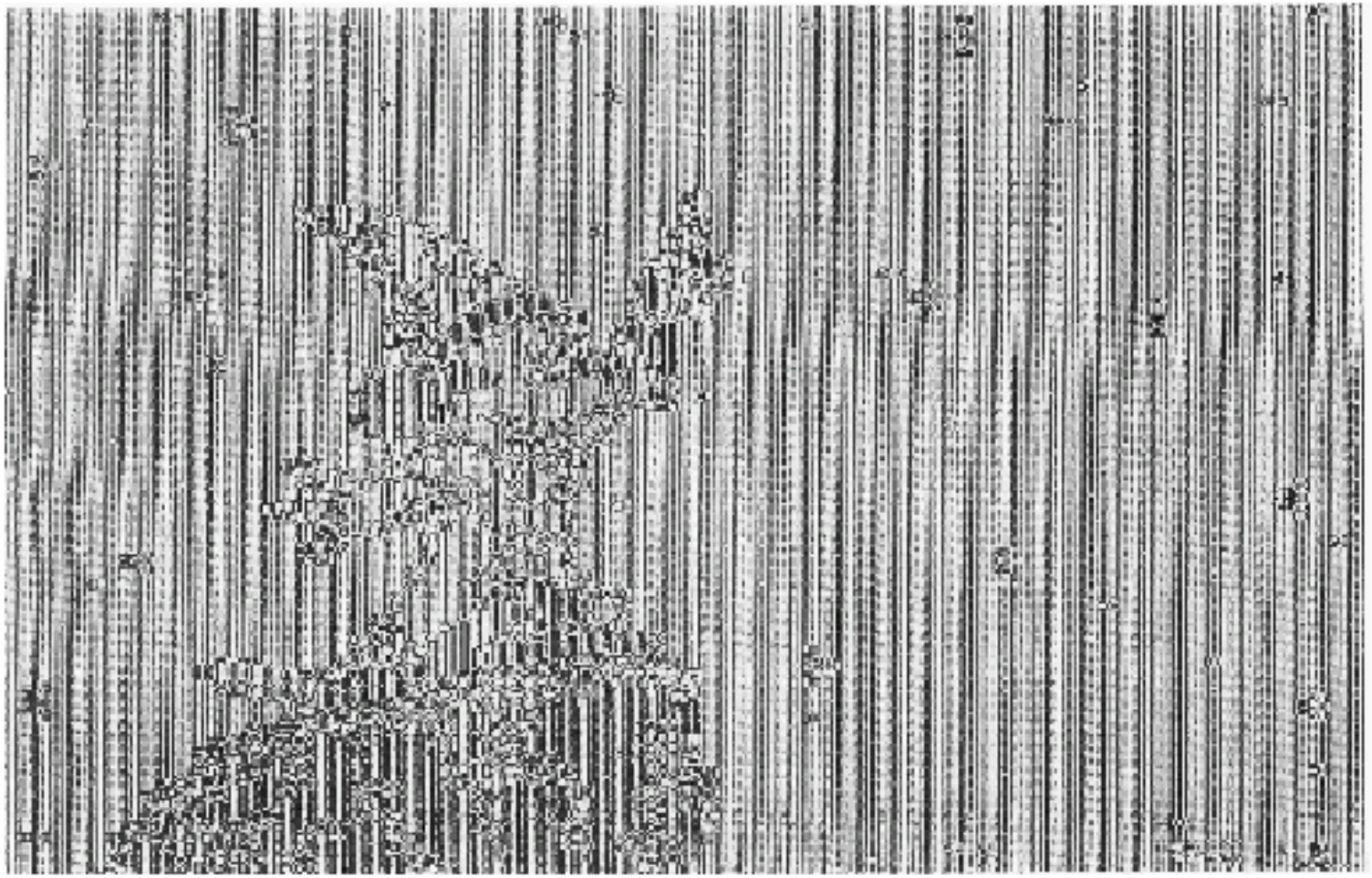
- Same plaintext block (b1 or b2) maps to same ciphertext block (c1 or c2)
  - Reordering is possible
- No error propagation
  - Bit changes only; bit deletions/omissions are a problem

EXAMPLE: MICKEY MOUSE



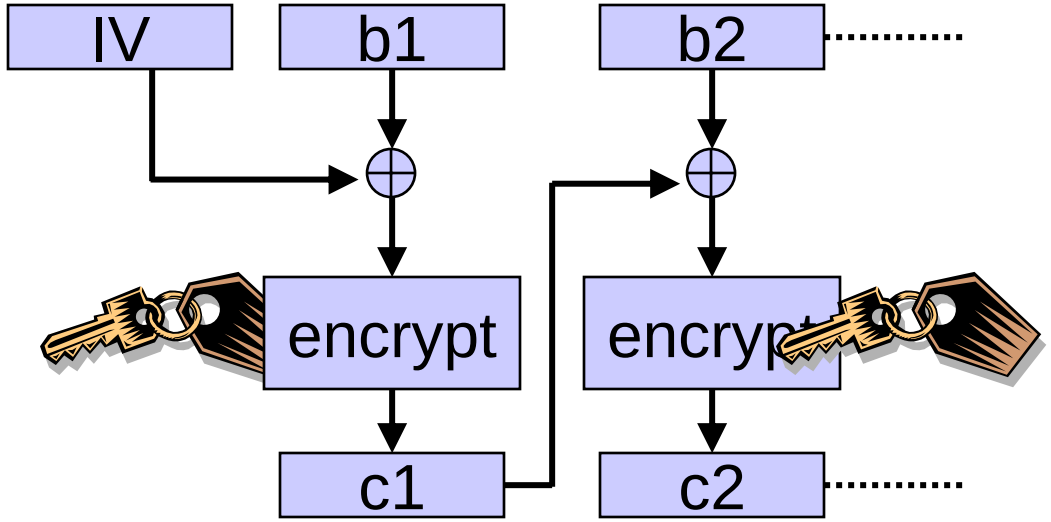
- Original picture

EXAMPLE: MICKEY MOUSE



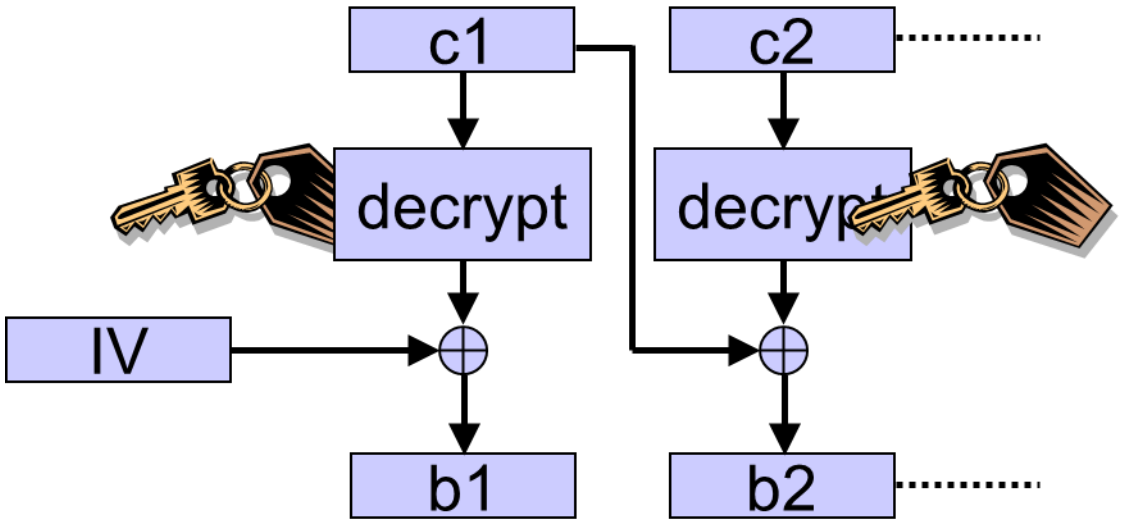
- Encrypted in ECB mode

CBC MODE



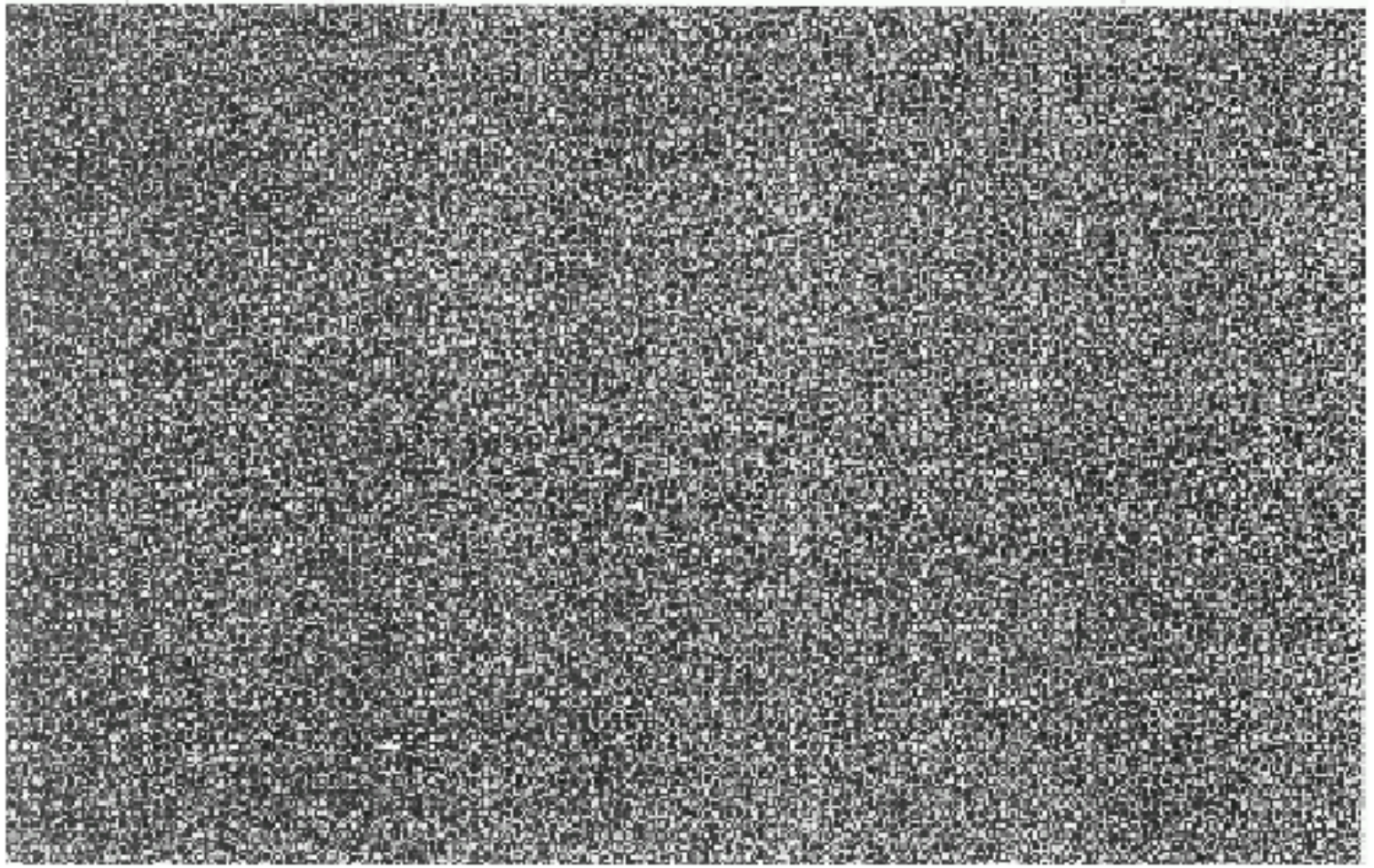
- Same plaintext block (b1 or b2) maps to different ciphertext block (c1 or c2)
  - Reordering is not possible
  - Depends on previous block

CBC MODE: ERROR PROPAGATION



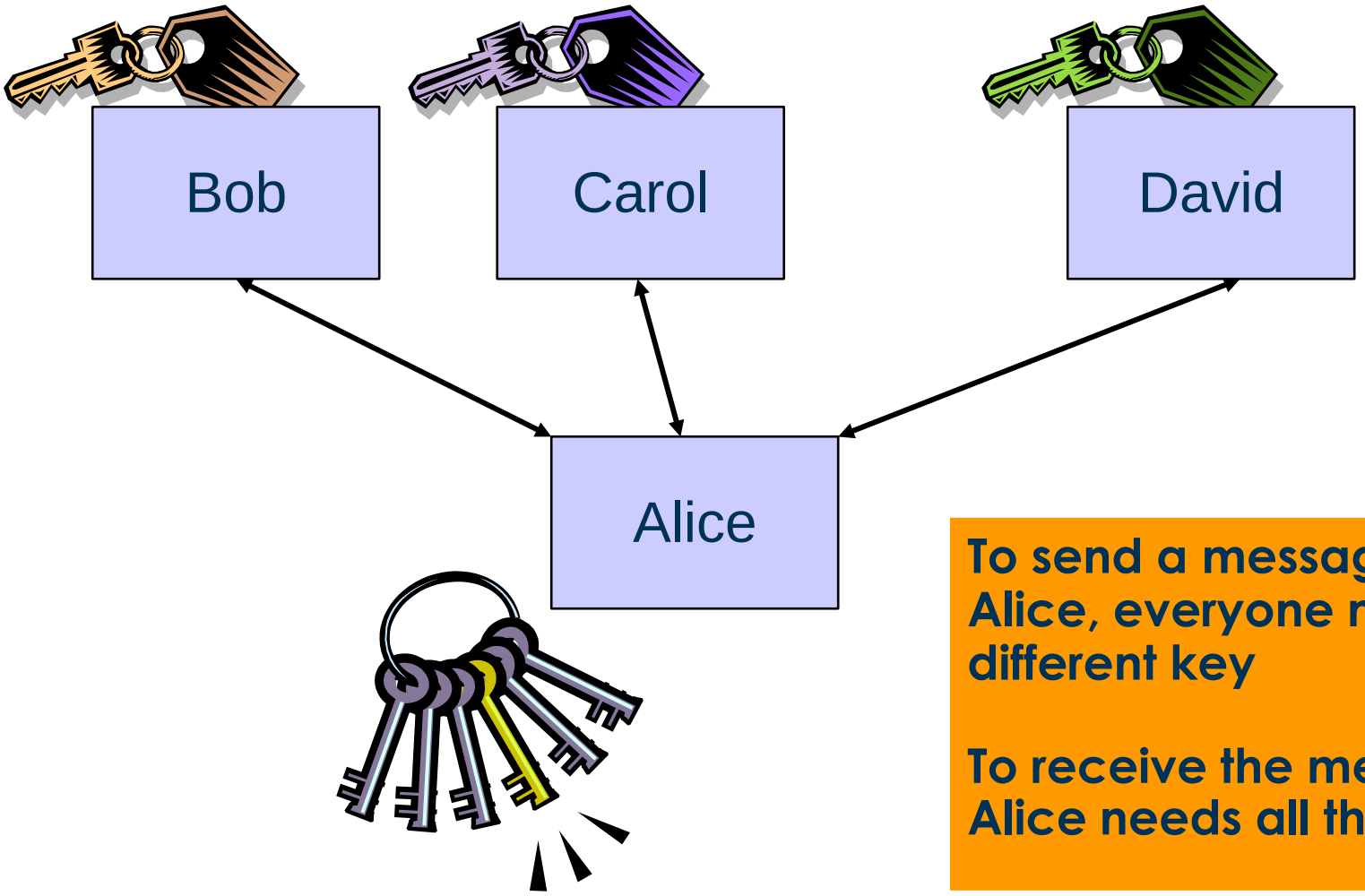
- Limited error propagation in case if ciphertext is modified or corrupted
  - Affects only current and next blocks

EXAMPLE: MICKEY MOUSE



- Encrypted in CBC mode

ISSUE: MANY SYMMETRIC KEYS



To send a message to Alice, everyone needs a different key

To receive the message, Alice needs all these keys

SUMMARY

- Modern ciphers are based on confusion and diffusion
- There are different modes of operation for encrypting large messages
- Scalability is the main issue in case of symmetric encryption

RESOURCES

- Read Chapter 2 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

Questions?

Thanks for your attention!