Questions

“What was that about bits of security / bits of key?”

Bits of key = (size of) the number of possible keys

Bits of security = (size of) the number of steps to break the cipher

Monoalphabetic substitution cipher:
- 26! possible keys
- far fewer steps to break the cipher

Weakness in the **cryptography** allows us to take shortcuts

Decrypting Vigenére

```
Key:    SECRETSECRE
Cipher: VICIQKSKGEX
```

```
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
F FGHIJKLMNOPQRSTUVWXYZABCDE
G GHIJKLMNOPQRSTUVWXYZABCDEF
  ...
```

Decrypting Vigenére

```
Key:    SECRETSECRE
Cipher: VICIQKSKGEX
```

```
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
F FGHIJKLMNOPQRSTUVWXYZABCDE
G GHIJKLMNOPQRSTUVWXYZABCDEF
  ...
```

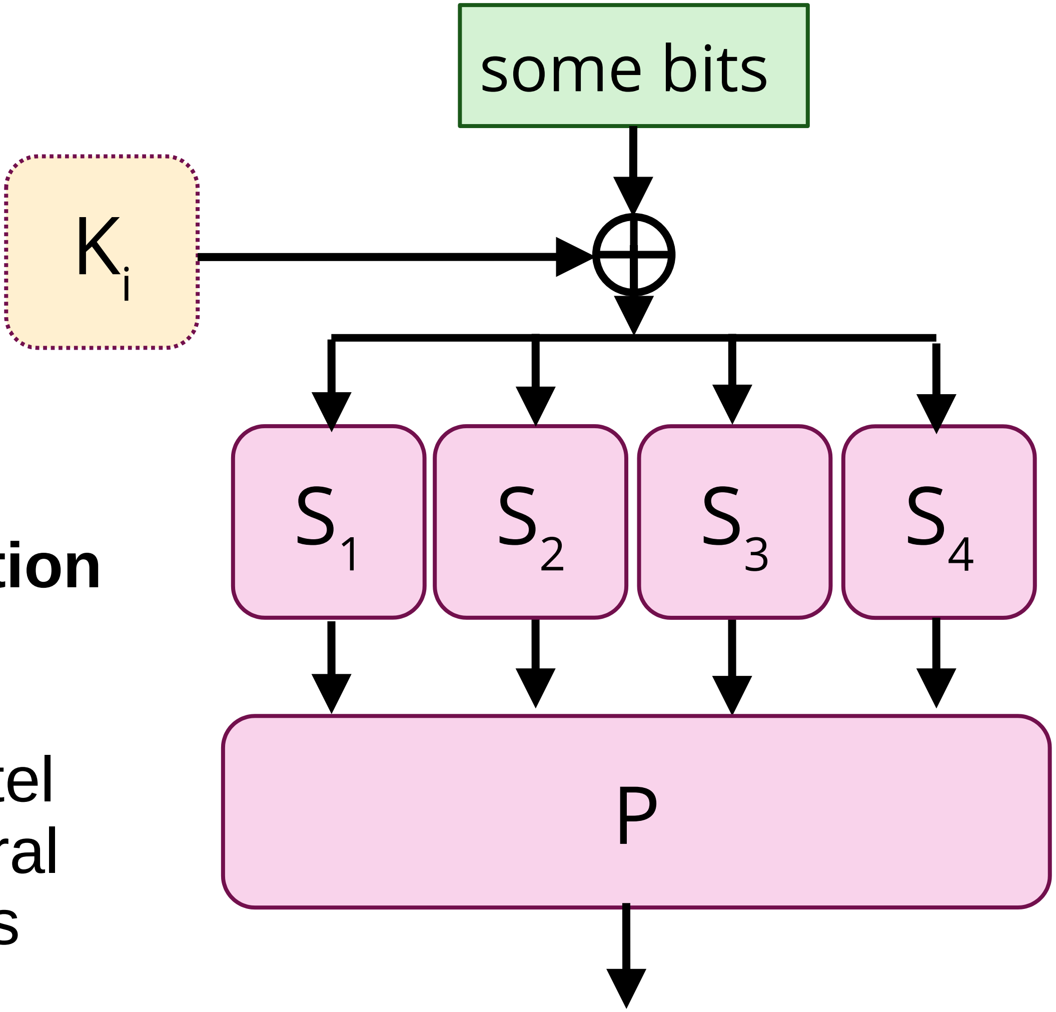
“I don't understand how AES works, could you please explain it in text?”

1. This thing →
is **not** AES.

AES is a particular block cipher

AES is a type of **substitution-permutation network**

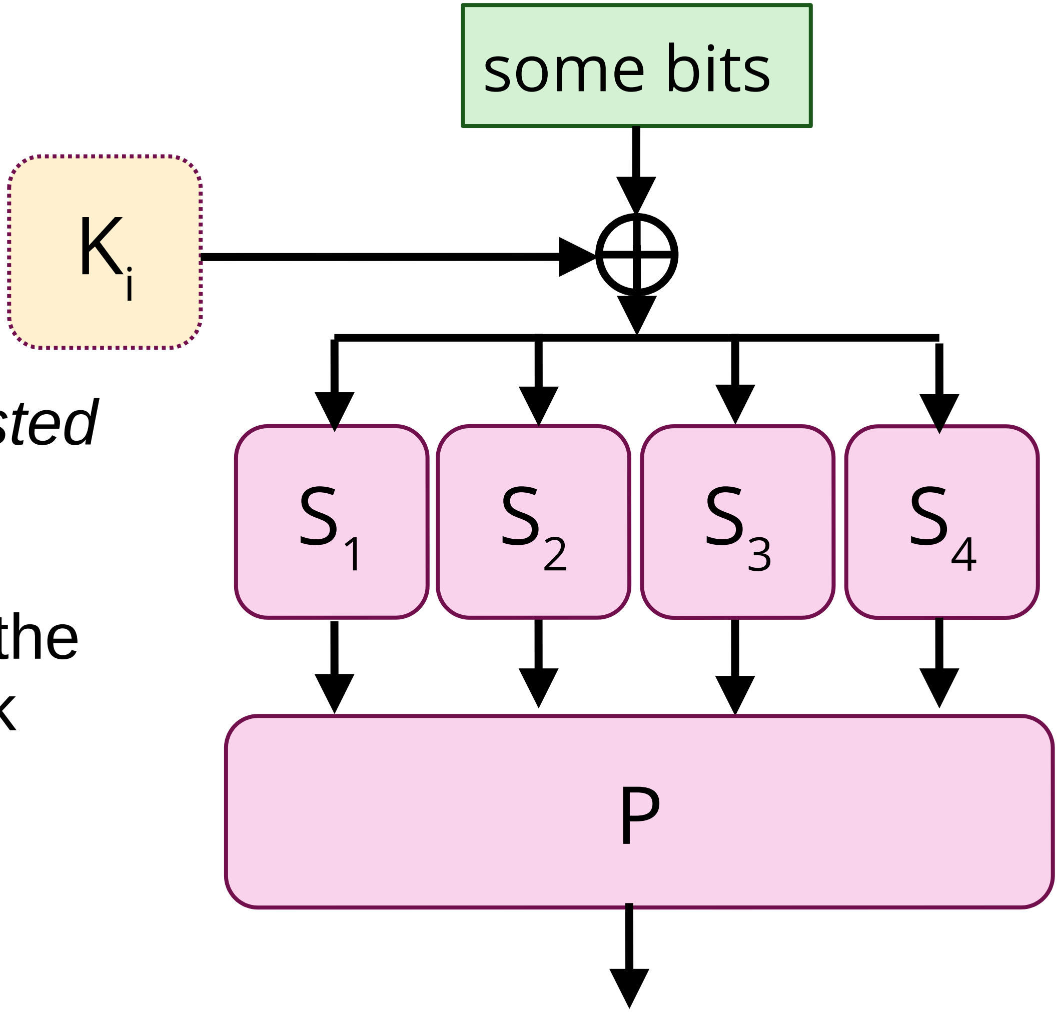
S-P networks and Feistel networks are two general classes of block ciphers



“I don't understand how AES works, could you please explain it in text?”

We’re not covering the core details of particular modern ciphers like AES in these lectures *(unless requested for a free session)*

Just an introduction to the common **types** of block ciphers



“I don't understand how AES works, could you please explain it in text?”

Key takeaways:

1. *Feistel networks* are a class of block ciphers which involve, for each of *N* rounds:

- splitting each input block in two halves
- applying a **round function** (with subkey) to the latter half
- XORing the result of the round function with the first half
- concatenating the XOR result with the original latter half
- this becomes the input to the next round

Exactly what the round function is, and other details, depend on the particular block cipher

“I don't understand how AES works, could you please explain it in text?”

Key takeaways:

2. *Substitution-permutation networks* are a class of block ciphers which involve, for each of *N* rounds:

- combining the input block with the subkey **somehow**
- sending parts of the ciphertext through a series of **S-boxes** and **P-boxes** to disguise patterns it might contain
- The result becomes the input to the next round

Exactly how each S-box and P-box operate, and how they are laid out, and how the key is introduced, are all dependent on the particular block cipher.