## Week 3: Autokey ciphers, cribs, and block ciphers

Jay Daigle

Occidental College

September 14, 2017

Jay Daigle (Occidental College)

Week 3: Block Ciphers

September 14, 2017 1 / 27

Jay Daigle (Occidental College)

Week 3: Block Ciphers

◆□ > ◆□ > ◆臣 > ◆臣 > ─臣 -

### Cribs

### Definition

A crib is a known or guessed portion of the plaintext, which can be used to help cryptanalyze a ciphertext.

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □

# OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW Let's guess the word "the" is in the message somewhere.

- 3

< 日 > < 同 > < 三 > < 三 >

| Ciphertext: | 0 | 0 | F |   | Κ | А | Α | Q | W | Μ | Ρ | Q | U | М | Х |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key:        | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | V | Н | В | Р | D | W | Н | J | S | Т | Ι | Μ | В | F | Т |
| Ciphertext: | Ζ | Х | Υ | I | R | Κ | Т | Ζ | S | Р | G | Μ | G | Ρ | Κ |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | G | Q | U | Р | Κ | G | A | S | 0 | W | Ζ | Ι | Ν | I | G |
| Ciphertext: | Q | М | I | Ρ | L | С | Ν | W | Х | Κ | Е | Ν | Q | L | D |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | X | F | Е | W | Е | Υ | U | Ρ | Т | R | Х | J | Х | Е | Ζ |
| Ciphertext: | Ι | R | F | S | Ν | I | J | А | Μ | G | Ρ | W |   |   |   |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |   |   |   |
| Plaintext:  | P | Κ | В | Z | G | Е | Q | Т | Ι | N | Ι | S |   |   |   |

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ▶ ● □

| Ciphertext: | 0 | 0 | F |   | Κ | А | Α | Q | W | M | Ρ | Q | U | М | Х |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key:        | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | V | Н | В | Р | D | W | Н | J | S | Т | T | Μ | В | F | Т |
| Ciphertext: | Ζ | Х | Υ | I | R | Κ | Т | Ζ | S | Р | G | Μ | G | Ρ | Κ |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | G | Q | U | Ρ | Κ | G | Α | S | 0 | W | Ζ | Ι | Ν | Ι | G |
| Ciphertext: | Q | М | I | Р | L | С | Ν | W | Х | K | Е | Ν | Q | L | D |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | T | Н | Е | Т | Н | Е |
| Plaintext:  | X | F | Е | W | Е | Υ | U | Ρ | Т | R | Х | J | Х | Е | Ζ |
| Ciphertext: | Ι | R | F | S | Ν | I | J | А | Μ | G | Ρ | W |   |   |   |
| Key:        | T | Н | Е | T | Н | Е | Т | Н | Е | T | Н | Е |   |   |   |
| Plaintext:  | P | Κ | В | Z | G | Е | Q | Т | Ι | N | Ι | S |   |   |   |

(日) (部) (注) (日) (三)

| Ciphertext: | 0 | 0 | F |   | Κ | А | Α | Q | W | M | Ρ | Q | U | Μ | Х |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key:        | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | V | Н | В | Р | D | W | Н | J | S | Т | T | Μ | В | F | Т |
| Ciphertext: | Ζ | Х | Υ | I | R | Κ | Т | Ζ | S | Р | G | Μ | G | Ρ | Κ |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |
| Plaintext:  | G | Q | U | Р | Κ | G | Α | S | 0 | W | Ζ | Ι | Ν | Ι | G |
| Ciphertext: | Q | Μ | I | Р | L | С | Ν | W | Х | K | Е | Ν | Q | L | D |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | T | Н | Е | Т | Н | Е |
| Plaintext:  | X | F | Е | W | Е | Υ | U | Ρ | Т | R | Х | J | Х | Е | Ζ |
| Ciphertext: | Ι | R | F | S | Ν | I | J | Α | Μ | G | Ρ | W |   |   |   |
| Key:        | T | Н | Е | Т | Н | Е | Т | Н | Е | Т | Н | Е |   |   |   |
| Plaintext:  | P | Κ | В | Z | G | Е | Q | Т | Ι | N | Ι | S |   |   |   |

Let's assume the "aso" was real and see what we can conclude.

- 34

< ロ > < 同 > < 回 > < 回 >

### Key Length of Four

### Key Length of Four

| 00F | IKA | AQW | MPQ | UMX | ZXY | IRK | TZS | PGM           | GPK | QMI | PLC | NWX | KEN | QLD |
|-----|-----|-----|-----|-----|-----|-----|-----|---------------|-----|-----|-----|-----|-----|-----|
| IRF | SNI | JAM | GPW |     |     |     |     |               |     |     |     |     |     |     |
|     |     |     |     |     | f   | bn- | the | -as           | 0   |     |     |     |     |     |
|     |     |     |     |     | t.  | he- | aso | - <b>σ</b> 11 | s   |     |     |     |     |     |
|     |     |     |     |     | Ū   |     | 400 | 6 <b>u</b>    | ~   |     |     |     |     |     |

## Key Length of Four

| 00F | IKA | AQW | MPQ | UMX | ZXY | IRK | TZS | PGM | GPK | QMI | PLC | NWX | KEN | QLD |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| IRF | SNI | JAM | GPW |     |     |     |     |     |     |     |     |     |     |     |
|     |     |     |     |     | f   | bn- | the | -as | o   |     |     |     |     |     |
|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|     |     |     |     |     | t   | he- | aso | -gu | s   |     |     |     |     |     |
|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |

"fbn" isn't very likely.

イロト 不得 とうせい かほとう ほ

### Key Length of Five

## Key Length of Five

| 00F | IKA | AQW | MPQ | UMX | ZXY | IRK | TZS | PGM | GPK | QMI | PLC | NWX | KEN | QLD |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| IRF | SNI | JAM | GPW |     |     |     |     |     |     |     |     |     |     |     |
|     |     |     |     |     | -er | e   | the | a   | so- |     |     |     |     |     |
|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|     |     |     |     |     | -th | e   | aso | m   | ob- |     |     |     |     |     |

## Key Length of Five

| 00F | IKA | AQW | MPQ | UMX | ZXY | IRK | TZS | PGM | GPK | QMI | PLC | NWX | KEN | QLD |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| IRF | SNI | JAM | GPW |     |     |     |     |     |     |     |     |     |     |     |
|     |     |     |     |     | -er | e   | the | a   | so- |     |     |     |     |     |
|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
|     |     |     |     |     | -th | e   | aso | m   | ob- |     |     |     |     |     |
|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |

This looks better...

- 3

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

## Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW ono --m di- -er e-- the --a so- -mo b-- auo --mdi --e re- -th e-- aso --m ob- -au o-- ncj --- ---\_\_\_

This looks better...but this doesn't.

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ● ● ● ● ● ● ●

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD TRF SNT JAM GPW gqu --- the --- aso --- the --- aso --- gxw

∃ <\0<</p>

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD TRF SNT JAM GPW gqu --- the --- aso --- the --- aso --- gxw

"gxw" and "gqu" both look bad.

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ● ● ● ● ● ● ●

 OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD

 IRF SNI JAM GPW

 --- --- --- gqu ---- the --- aso --- --- --- -- 

 --- --- --- --- the --- aso --- gxw --- --- --- -- 

"gxw" and "gqu" both look bad.

We could keep trying longer keywords. We won't get anywhere.

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ● ● ● ● ● ● ●

### A new offset?

| Ciphertext: | 0 | 0 | F | Ι | Κ | A | А | Q | W | М | Ρ | Q | U | М | Х |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key:        | - | - | Т | Н | Е | T | Н | Е | Т | Н | Е | Т | Н | Е | Т |
| Plaintext:  | - | - | Μ | В | G | H | Т | М | D | F | L | X | Ν | Ι | E |
| Ciphertext: | Ζ | Х | Y | I | R | K | Т | Ζ | S | Ρ | G | М | G | Ρ | K |
| Key:        | H | Е | Т | Н | Е | T | Н | Е | Т | Н | Е | Т | Н | Е | Т |
| Plaintext:  | S | Т | F | В | Ν | R | Μ | V | Ζ | Ι | С | Т | Ζ | L | R |
| Ciphertext: | Q | М | Ι | Ρ | L | С | Ν | W | Х | Κ | Е | Ν | Q | L | D |
| Key:        | H | Е | Т | Н | Е | T | Н | Е | Т | Н | Е | Т | Н | Е | Т |
| Plaintext:  | J | Ι | Р | Ι | Н | J | G | S | E | D | А | U | J | Н | K |
| Ciphertext: | Ι | R | F | S | Ν | Ι | J | А | Μ | G | Ρ | W |   |   |   |
| Key:        | H | Е | Т | Н | Е | T | Н | Е | Т | Н | Е | Т |   |   |   |
| Plaintext:  | В | Ν | Μ | L | J | P | С | W | Т | Ζ | L | D |   |   |   |

### A new offset?

| Ciphertext: | 0 | 0 | F | Ι | Κ | A | А | Q | W | М | Ρ | Q | U | М | Х |
|-------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key:        | - | - | Т | Н | Е | T | Н | Е | Т | Н | Е | Т | Н | Е | Т |
| Plaintext:  | - | - | Μ | В | G | H | Т | М | D | F | L | X | Ν | Ι | Е |
| Ciphertext: | Ζ | Х | Y | I | R | K | Т | Ζ | S | Ρ | G | М | G | Ρ | K |
| Key:        | H | Е | Т | Н | Е | T | Н | Е | Т | Н | Е | Т | Н | Е | Т |
| Plaintext:  | S | Т | F | В | Ν | R | Μ | V | Ζ | Ι | С | Т | Ζ | L | R |
| Ciphertext: | Q | М | Ι | Ρ | L | С | Ν | W | Х | Κ | Е | Ν | Q | L | D |
| Key:        | H | Е | Т | Н | Е | T | Н | Е | Т | Н | Е | Т | Н | Е | Т |
| Plaintext:  | J | Ι | Р | Ι | Н | J | G | S | E | D | А | U | J | Н | K |
| Ciphertext: | Ι | R | F | S | Ν | Ι | J | А | Μ | G | Ρ | W |   |   |   |
| Key:        | H | Е | Т | Н | Е | T | Н | Е | Т | Н | Е | Т |   |   |   |
| Plaintext:  | В | Ν | Μ | L | J | P | С | W | Т | Ζ | L | D |   |   |   |

### Key Length of Four

### Key Length of Four

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW -- -wj q-t he- est --- ----- -th e-e st- ezr \_\_\_

10 / 27

## Key Length of Four

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW -- -wj q-t he- est --- ----- -th e-e st- ezr

Nope.

10 / 27

### Key Length of Five

◆ロ > ◆母 > ◆臣 > ◆臣 > ○ 臣 ○ のへで

### Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW --- tim --t he- -es t-- --the --e st- -ns a-- ---

## Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW --- tim --t he- -es t-- ------ the --e st- -ns a-- --- ---

Promising....

## Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW --s o-- tim --t he- -es t-- nsa \_\_\_ so- --i m-- the --e st- -ns a-- com

Promising....

## Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h ea- -we r-- res so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w er- -re s-- ple

Promising....And now it's a fill-in-the-blank puzzle.

## Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h ea- -we r-- res so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w er- -re s-- ple

Promising....And now it's a fill-in-the-blank puzzle.

## Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h ea- -we r-- res so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w er- -re sim ple

Promising....And now it's a fill-in-the-blank puzzle.

### Key Length of Five

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW wat ers ome tim est heq ues tio nsa rec omp lic ate dan dth ean swe rsa res som eti mes the que sti ons are com pli cat eda ndt hea nsw ers are sim ple

Done!

# "Sometimes the questions are complicated, and the answers are simple." Theodor Geisel

### "Sometimes the questions are complicated, and the answers are simple." Theodor Geisel a.k.a. Dr. Seuss

Jay Daigle (Occidental College)

Week 3: Block Ciphers

September 14, 2017

17 / 27
#### Definition

A block cipher encrypts fixed-sized blocks of ciphertext, rather than single letters at a time.

Jay Daigle (Occidental College)

Week 3: Block Ciphers

◆ロ > ◆母 > ◆臣 > ◆臣 > ○日 ○ ○ ○ ○ September 14, 2017

18 / 27

#### Permutation cipher

We choose a block size n, and as a key choose an element  $k \in S_n$ , which is a permutation on an alphabet of n letters.

# Permutation cipher

We choose a block size n, and as a key choose an element  $k \in S_n$ , which is a permutation on an alphabet of n letters.

To encrypt, we break our plaintext into blocks of size n, padding the final block with nonsense characters if necessary. Then we permute each block according to the key k.

# Permutation cipher

We choose a block size n, and as a key choose an element  $k \in S_n$ , which is a permutation on an alphabet of n letters.

To encrypt, we break our plaintext into blocks of size n, padding the final block with nonsense characters if necessary. Then we permute each block according to the key k.

To decrypt, we take the inverse permutation  $k^{-1}$  and apply this to each ciphertext block.

18 / 27

Jay Daigle (Occidental College)

Week 3: Block Ciphers

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

"Fourscore and seven years ago"

< 同 ▶

"Fourscore and seven years ago"

Block size five

< 17 ▶

```
"Fourscore and seven years ago"
```

3

```
"Fourscore and seven years ago"
```

fours corea ndsev enyea rsago

3

```
"Fourscore and seven years ago"
```

```
Block size five and key k = (12345) \mapsto (23514).
```

fours corea ndsev enyea rsago

RFOSU

< ∃ →

```
"Fourscore and seven years ago"
```

fours corea ndsev enyea rsago

RFOSU

< ∃ →

```
"Fourscore and seven years ago"
```

fours corea ndsev enyea rsago

RFOSU

< ∃ →

```
"Fourscore and seven years ago"
```

fours corea ndsev enyea rsago

RFOSU

< ∃ →

```
"Fourscore and seven years ago"
```

fours corea ndsev enyea rsago

RFOSU

< ∃ →

```
"Fourscore and seven years ago"
```

fours corea ndsev enyea rsago

RFOSU

< ∃ →

```
"Fourscore and seven years ago"
```

```
Block size five and key k = (12345) \mapsto (23514).
```

fours corea ndsev enyea rsago

RFOSU ECOAR ENDVS EENAY GRSOA.

3

Jay Daigle (Occidental College)

Week 3: Block Ciphers

▲ロト ◆ ● ト ◆ ● ト ◆ ● ト ● ● 今 Q ○
September 14, 2017 20 / 27

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \left( \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Jay Daigle (Occidental College)

Week 3: Block Ciphers

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへで September 14, 2017

20 / 27



æ

21 / 27

<ロ> <同> <同> < 同> < 同>



Lester Hill's patented cipher machine

э

< 合

Э

21 / 27

Jay Daigle (Occidental College)

Week 3: Block Ciphers

< □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □ ▶ < □

## Hill Cipher

We first choose a block size *n*. We choose a key, which is a  $n \times n$  matrix *K* with entries in  $\mathbb{Z}/26\mathbb{Z}$  (that is, integers modulo 26). We require that gcd(26, det K) = 1.

We divide our message into blocks of length *n*. We write each plaintext block as a column vector  $B \in (\mathbb{Z}/26\mathbb{Z})^n$ . The corresponding ciphertext block is given by *KB*.

To decrypt, we compute  $K^{-1}$  in  $\mathbb{Z}/26\mathbb{Z}$ . Given a ciphertext block *C*, the corresponding plaintext block is  $K^{-1}C$ .

22 / 27

Jay Daigle (Occidental College)

Week 3: Block Ciphers

▲ロト ◆ □ ト ◆ 三 ト ◆ 三 ト ● 三 少 へ ○
September 14, 2017 23 / 27

æ

(日)

IT WA SA DA RK AN DS TO RM YN IG HT

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K\begin{bmatrix} 8\\19\end{bmatrix} = \begin{bmatrix} 43\\78\end{bmatrix} \equiv \begin{bmatrix} 17\\0\end{bmatrix}$$

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$\mathcal{K}\begin{bmatrix}8\\19\end{bmatrix} = \begin{bmatrix}43\\78\end{bmatrix} \equiv \begin{bmatrix}17\\0\end{bmatrix} \qquad \qquad \mathcal{K}\begin{bmatrix}22\\0\end{bmatrix} = \begin{bmatrix}66\\110\end{bmatrix} \equiv \begin{bmatrix}14\\6\end{bmatrix}$$

э

24 / 27

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$\mathcal{K} \begin{bmatrix} 8\\19 \end{bmatrix} = \begin{bmatrix} 43\\78 \end{bmatrix} \equiv \begin{bmatrix} 17\\0 \end{bmatrix}$$
$$\mathcal{K} \begin{bmatrix} 18\\0 \end{bmatrix} = \begin{bmatrix} 54\\90 \end{bmatrix} \equiv \begin{bmatrix} 2\\12 \end{bmatrix}$$

$$\mathcal{K}\begin{bmatrix}22\\0\end{bmatrix} = \begin{bmatrix}66\\110\end{bmatrix} \equiv \begin{bmatrix}14\\6\end{bmatrix}$$

э

24 / 27

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$\mathcal{K} \begin{bmatrix} 8\\19 \end{bmatrix} = \begin{bmatrix} 43\\78 \end{bmatrix} \equiv \begin{bmatrix} 17\\0 \end{bmatrix} \qquad \qquad \mathcal{K} \begin{bmatrix} 22\\0 \end{bmatrix} = \begin{bmatrix} 66\\110 \end{bmatrix} \equiv \begin{bmatrix} 14\\6 \end{bmatrix} \\ \mathcal{K} \begin{bmatrix} 18\\0 \end{bmatrix} = \begin{bmatrix} 54\\90 \end{bmatrix} \equiv \begin{bmatrix} 2\\12 \end{bmatrix} \qquad \qquad \mathcal{K} \begin{bmatrix} 3\\0 \end{bmatrix} = \begin{bmatrix} 9\\15 \end{bmatrix} \equiv \begin{bmatrix} 9\\15 \end{bmatrix}$$

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$\mathcal{K} \begin{bmatrix} 8\\19 \end{bmatrix} = \begin{bmatrix} 43\\78 \end{bmatrix} \equiv \begin{bmatrix} 17\\0 \end{bmatrix} \qquad \qquad \mathcal{K} \begin{bmatrix} 22\\0 \end{bmatrix} = \begin{bmatrix} 66\\110 \end{bmatrix} \equiv \begin{bmatrix} 14\\6 \end{bmatrix} \\ \mathcal{K} \begin{bmatrix} 18\\90 \end{bmatrix} = \begin{bmatrix} 54\\90 \end{bmatrix} \equiv \begin{bmatrix} 2\\12 \end{bmatrix} \qquad \qquad \mathcal{K} \begin{bmatrix} 3\\0 \end{bmatrix} = \begin{bmatrix} 9\\15 \end{bmatrix} \equiv \begin{bmatrix} 9\\15 \end{bmatrix}$$

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$\mathcal{K} \begin{bmatrix} 8\\19 \end{bmatrix} = \begin{bmatrix} 43\\78 \end{bmatrix} \equiv \begin{bmatrix} 17\\0 \end{bmatrix} \qquad \qquad \mathcal{K} \begin{bmatrix} 22\\0 \end{bmatrix} = \begin{bmatrix} 66\\110 \end{bmatrix} \equiv \begin{bmatrix} 14\\6 \end{bmatrix} \\ \mathcal{K} \begin{bmatrix} 18\\90 \end{bmatrix} = \begin{bmatrix} 54\\90 \end{bmatrix} \equiv \begin{bmatrix} 2\\12 \end{bmatrix} \qquad \qquad \mathcal{K} \begin{bmatrix} 3\\0 \end{bmatrix} = \begin{bmatrix} 9\\15 \end{bmatrix} \equiv \begin{bmatrix} 9\\15 \end{bmatrix}$$

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

RA OG CM JP JA NA BZ TT LF HQ EA OV

Jay Daigle (Occidental College)

Week 3: Block Ciphers

▲□▶ ▲□▶ ▲ ■ ▶ ▲ ■ ▶ ▲ ■ かへで September 14, 2017 25 / 27 how are you today

イロン イロン イヨン イヨン

how are you today

ZWS ENI USP LJVEU
how are you today

ZWS ENI USP LJVEU

07-14 22-00 17-04 24-14 20-19 14-03 00-24

Jay Daigle (Occidental College)

Week 3: Block Ciphers

September 14, 2017

3

25 / 27

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

how are you today

ZWS ENI USP LJVEU

07-14 22-00 17-04 24-14 20-19 14-03 00-24

25-22 18-08 13-08 20-18 15-11 09-21 04-20

Jay Daigle (Occidental College)

Week 3: Block Ciphers

A B + A B + September 14, 2017 25 / 27

- 34

Jay Daigle (Occidental College)

Week 3: Block Ciphers

▲ロト ◆ ● ト ◆ ● ト ◆ ● ト ● ● 今 Q ○
September 14, 2017 26 / 27



# Claude Shannon

## Picture CC BY-SA 2.0 de by Konrad Jacobs

Jay Daigle (Occidental College)

Week 3: Block Ciphers

September 14, 2017

э

э

< 同 ▶

26 / 27

Jay Daigle (Occidental College)

Week 3: Block Ciphers

▲ロト ◆ □ ト ◆ 三 ト ◆ 三 ト 三 少 へ ○
September 14, 2017 27 / 27

### Definition

An encryption method has good diffusion if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

### Definition

An encryption method has good diffusion if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

#### Definition

An encryption method has good confusion if the key does not relate straightforwardly to the ciphertext, but each part of the ciphertext depends on many parts of the key.

27 / 27