# Lecture 5.1: Basic cryptographic ciphers

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

# Encoding messages as numbers

In this lecture, we'll see how to send encoded messages, which will be numbers.

We can encode any word as a number in base-26:

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

In base 26, the word **CLEMSON** can be encoded as 2 11 4 12 18 14 13.

We can convert this to decimal (base 10):

$$2 \cdot 26^0 + 11 \cdot 26^1 + 4 \cdot 26^2 + 12 \cdot 26^3 + 18 \cdot 26^4 + 14 \cdot 26^5 + 13 \cdot 26^6 = 4190683824.$$

To reverse this process, recursively divide 26 into the number. Let's try this with 221707947:

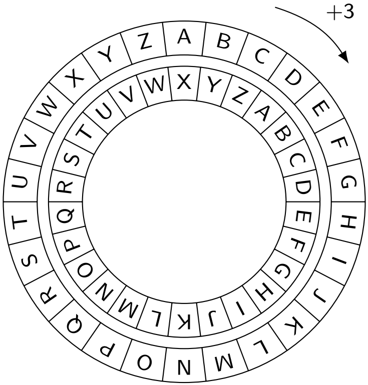
$$\begin{array}{rcrcrl}
221707947 & = & 8527228 \cdot 26 & + & 19 & \quad \mathbf{T} \\
8527228 & = & 327970 \cdot 26 & + & 8 & \quad \mathbf{I} \\
327970 & = & 12614 \cdot 26 & + & 6 & \quad \mathbf{G} \\
12614 & = & 485 \cdot 26 & + & 4 & \quad \mathbf{E} \\
485 & = & 18 \cdot 26 & + & 17 & \quad \mathbf{R} \\
18 & = & 0 \cdot 26 & + & 18 & \quad \mathbf{S}
\end{array}$$

Now, suppose that we wanted to send this as a secret message. . .

# Some history

Though he wasn't the first, Julius Caesar (100 B.C–44 B.C) used an encryption device called a cipher in his private correspondences.

An encrypted message would looks something like this: **RZ WKDWV VKDUS**




Decrypted message: **OW THATS SHARP**

# Caesar cipher

The Caesar cipher is defined by the following:

- key, $k \in N$,
- encryption function, $e(x)$,
- decryption function, $d(x)$,

$$e(x) = x + k \pmod{26}, \qquad d(y) = y - k \pmod{26}.$$

We first associate each letter to a number in $\mathbb{Z}_{26} := \{0, 1, \ldots, 24, 25\}$, as follows:

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

To see an example of this, suppose that $k = 18$.

We encrypt the letter **R** by

$$\begin{aligned} e(17) &\equiv 17 + 18 \pmod{26} \\ &\equiv 35 \pmod{26} \\ &\equiv 9 \pmod{26} \end{aligned}$$

which is **J**.

Let's decrypt **L**:

$$\begin{aligned} d(11) &\equiv 11 - 18 \pmod{26} \\ &\equiv -7 \pmod{26} \\ &\equiv 19 \pmod{26} \end{aligned}$$

which is **T**.

# A cipher with multiplication

Consider the following encryption function:

$$e\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \qquad e(x) = 5x \pmod{26}.$$

This works because the function $e$ is injective, and this is because $\gcd(26, 5) = 1$.

Let's encrypt the letter $R$, which is $x = 17$:

$$\begin{aligned} e(17) &\equiv 5 \cdot 17 \pmod{26} \\ &\equiv 85 \pmod{26} \\ &\equiv 7 \pmod{26}. \end{aligned}$$

The decryption function is

$$d(x) = 21x \pmod{26}.$$

This works because in $\mathbb{Z}_{26}$, the multiplicative inverse of $k = 5$ is $5^{-1} := 21$:

$$\begin{aligned} 5 \cdot 21 &\equiv 105 \pmod{26} \\ &\equiv 1 \pmod{26}. \end{aligned}$$

## Number theory fact

A number $k \in \mathbb{Z}_n$ has a multiplicative inverse iff $\gcd(n, k) = 1$.

# A cipher with multiplication and addition

Consider the following encrypting function:

$$e\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \qquad e(x) = 5x + 3 \pmod{26}.$$

In other words, given the input $x$, we:

1. multiply by 5
2. add 3.

To decrypt a message $m$, we need to "undo these" in the opposite order:

2. subtract 3
1. multiply by $5^{-1} = 21$.

The decryption function is thus

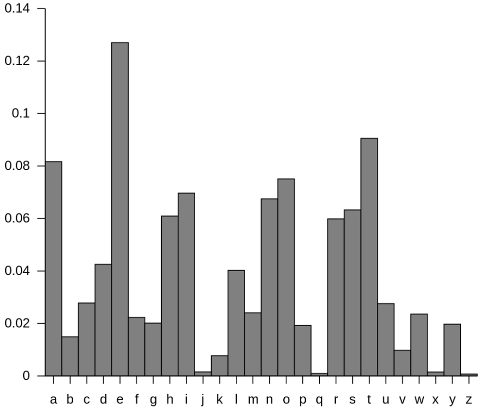
$$d(x) = 21(x - 3) \pmod{26}.$$

# A weakness of character ciphers

The ciphers that we've seen are called character, or monographic ciphers: all copies of the same letter get encrypted the same way:

$$e(x_i) = e(x_j) \ \Rightarrow x_i = x_j.$$

If the message is long, the the private key can be deduced by analyzing letter frequencies.



## Block ciphers

A more sophisticated cipher are the block, or polygraphic ciphers, which encrypt blocks of plaintext letters to blocks of ciphertext letters of the same length.

One such system was developed by Blaise de Vigenère in 1585, called the Vigenère cipher.

We'll introduce this by an example.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Let's encrypt the message **ENGINEERING**:

$$p_1 p_2 p_3 p_4 p_5 p_6 p_7 p_8 p_9 p_{10} p_{11} = 4\ \ 13\ \ 6\ \ 8\ \ 13\ \ 4\ \ 4\ \ 17\ \ 8\ \ 13\ \ 6$$

using the key **ROCKS**:

$$k_1 k_2 k_3 k_4 k_5 = 17\ \ 14\ \ 2\ \ 10\ \ 18.$$

| | **E** | **N** | **G** | **I** | **N** | **E** | **E** | **R** | **I** | **N** | **G** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $p_i$ | 4 | 13 | 6 | 8 | 13 | 4 | 4 | 17 | 8 | 13 | 6 |
| $k_i$ | 17 | 14 | 2 | 10 | 18 | 17 | 14 | 2 | 10 | 18 | 17 |
| $c_i = p_i + k_i$ | 21 | 1 | 8 | 18 | 5 | 21 | 18 | 19 | 18 | 5 | 23 |
| | **V** | **B** | **I** | **S** | **F** | **V** | **S** | **T** | **S** | **F** | **X** |

# Decryption with the Vigenère cipher

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Let's decrypt the message **TZGWK FBVSY WFU**:

$$c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8 c_9 c_{10} c_{11} c_{12} c_{13} = 19 \ \ 25 \ \ 6 \ \ 22 \ \ 10 \ \ 5 \ \ 1 \ \ 21 \ \ 18 \ \ 24 \ \ 22 \ \ 5 \ \ 20$$

using the same key **ROCKS**:

$$k_1 k_2 k_3 k_4 k_5 = 17 \ \ 14 \ \ 2 \ \ 10 \ \ 18.$$

| | **T** | **Z** | **G** | **W** | **K** | **F** | **B** | **V** | **S** | **Y** | **W** | **F** | **U** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $c_i$ | 19 | 25 | 6 | 22 | 10 | 5 | 1 | 21 | 18 | 24 | 22 | 5 | 20 |
| $k_i$ | 17 | 14 | 2 | 10 | 18 | 17 | 14 | 2 | 10 | 18 | 17 | 14 | 2 |
| $p_i = c_i - k_i$ | 2 | 11 | 4 | 12 | 18 | 14 | 13 | 19 | 8 | 6 | 4 | 17 | 18 |
| | **C** | **L** | **E** | **M** | **S** | **O** | **N** | **T** | **I** | **G** | **E** | **R** | **S** |

## Different types of ciphers

The ciphers in this lecture are symmetric: Decryption is the opposite ("inverse") of encryption.

Not only is the same key is used for encryption and decryption, but that key needs to be kept private.

### Definition

In an asymmetric cipher, there are two distinct keys:

- A public key, used for encryption;
- A private key, used for decryption.

The instructions for encrypting a meesage can be made public without compromising the security.