

# Simple Cryptography

Program kryptograficzny

Kacper Bojanowski, Filip Opiłka



# Czym jest Simple Cryptography?

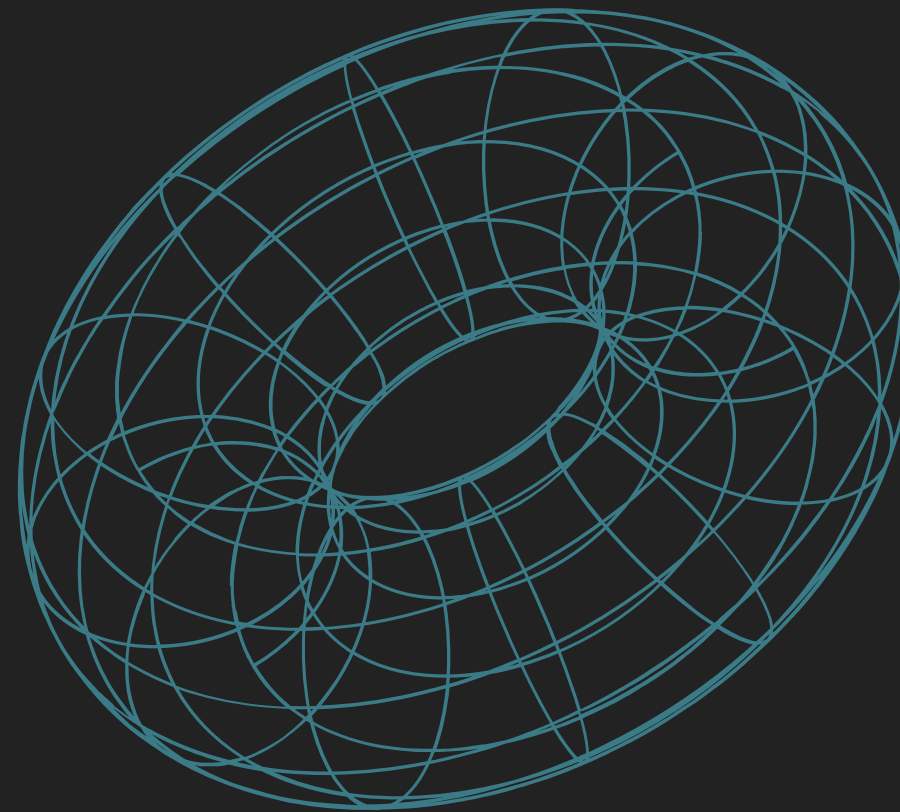
"Simple Cryptography" to aplikacja pozwalająca na zapoznanie się z działaniem kryptografii klasycznej, oraz innych zastosowań szyfrowania.



**Czemu temat kryptografia?**

Pozwala nam w bezpieczny  
sposób korzystać z internetu

Jest tajemnicza



Towarzyszy ludzkości od ponad  
3900 lat

Bez niej nie słyszelibyśmy tak  
często o Bitcoinie czy Blockchainie

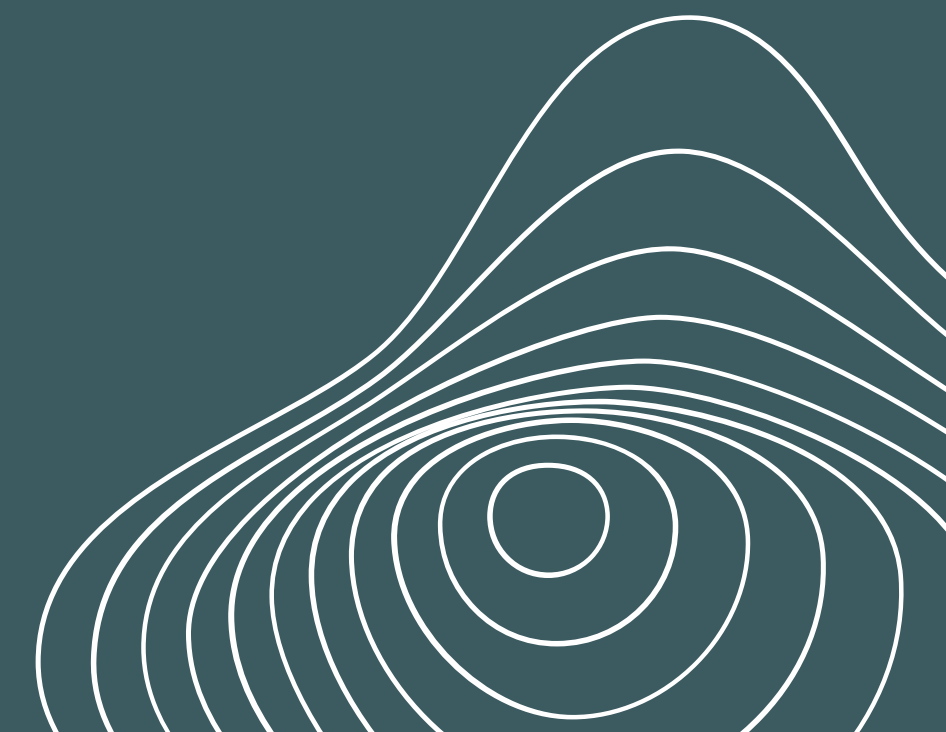


# **Kryptografia Klasyczna**

# ★★★★★ Szyfr Cezara

Szyfr podstawieniowy, będący jednym z najpopularniejszych szyfrów na świecie.

Jest bardzo prostym i szybkim sposobem zaszyfrowania wiadomości, podatnym na ataki alfabetyczne lub brute-force'a.



# Sposób szyfrowania

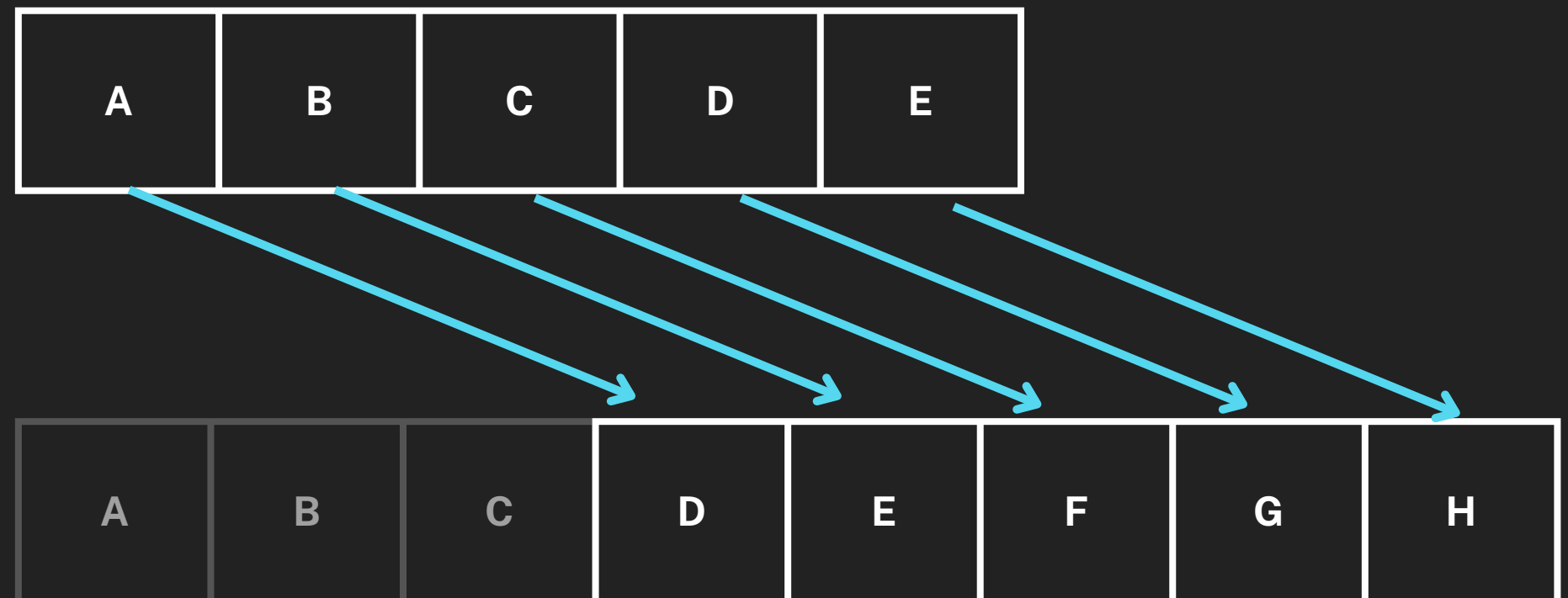
1

Klucz : 3

2

Szyfrowanie polega na zastąpieniu kolejnych liter tekstu jawnego literą oddaloną o stałą liczbę pozycji w alfabecie

A B C D E



D E F G H

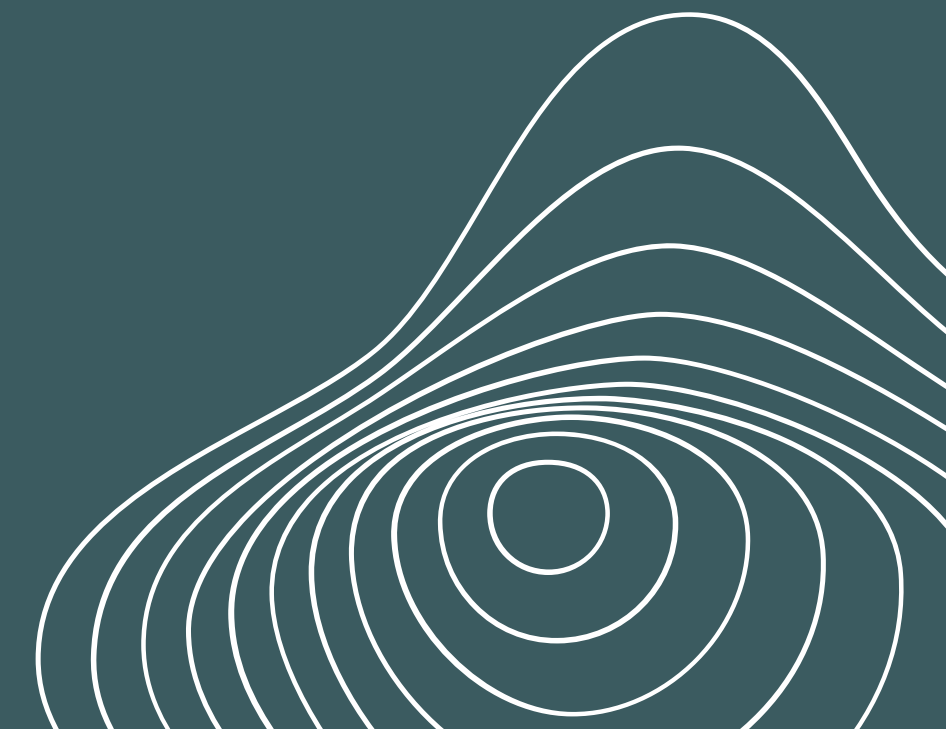




# ★★★★★ Szyfr Playfaira

Szyfr poligramowy wymyślony w 1854 roku  
przez Charlesa Wheatstone'a

Nazwa szyfru pochodzi od nazwiska lorda  
Lyona Playfaira, który przyczynił się do  
rozpowszechnienia szyfru





# Sposób szyfrowania

1

Klucz : KLUCZ



2

Tajna wiadomosc



**TA IN AW IA DO MO SC**



J zostaje zamienione na I

|   |   |   |   |   |
|---|---|---|---|---|
| K | L | U | C | Z |
| A | B | D | E | F |
| G | H | I | M | N |
| O | P | Q | R | S |
| T | V | W | X | Y |

## Zasady:

- Gdy parą są te same litery rozdziela się je literą "X" np. TT -> TX i XT
- Gdy tekst jawny jest nieparzysty na jego końcu dodajemy literę "Z"

3

# TA IN AW IA DO MO SC

Szukamy pary w macierzy:

## Zasady:

- Jeśli para liter jest w tej samej kolumnie wybieramy litery pod nimi ( TA -> KG )
- Jeśli para liter jest w tym samym wierszu wybieramy litery po ich prawej stronie ( IN -> MG )
- Jeśli para liter jest na przekątnych prostokąta wybieramy parę na drugiej przekątnej ( AW -> DT )

|   |   |   |   |   |
|---|---|---|---|---|
| K | L | U | C | Z |
| A | B | D | E | F |
| G | H | I | M | N |
| O | P | Q | R | S |
| T | V | W | X | Y |

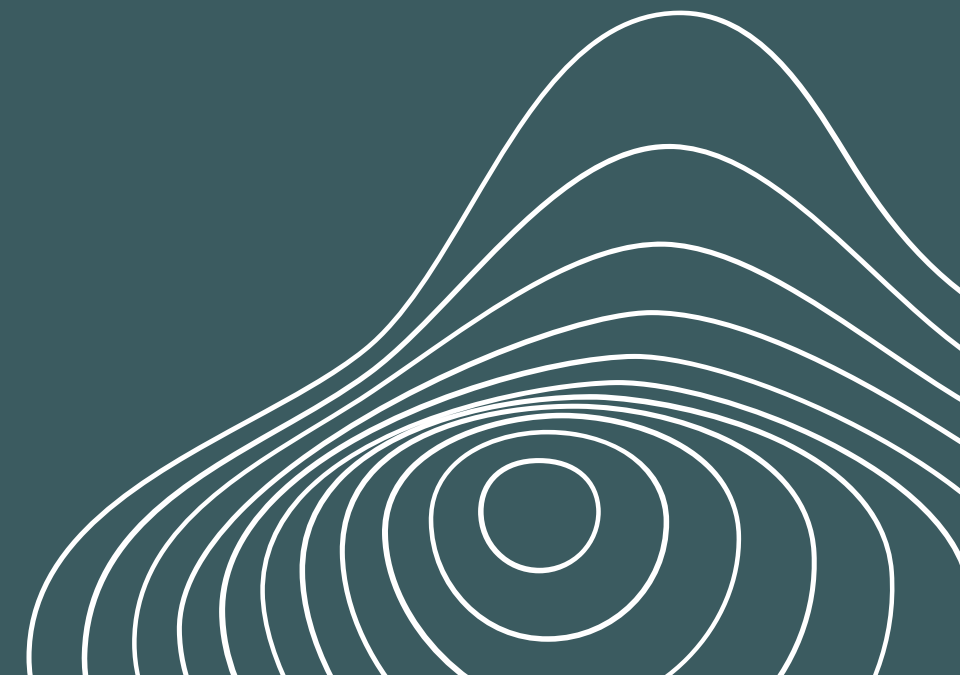
**KG MG DT GD AQ GR RZ**

# ★★★★★ Szyfr Vigenère

Polialfabetyczny szyfr podstawieniowy  
stworzony przez Blaise de Vigenere'a już w  
1586 roku.

Powstał na podstawie prostszego szyfru.

**Jakiego?**



# Sposób szyfrowania

1

Klucz : **KLUCZ**



**KLUCZKLUCZKLUC** 14 liter

**TAJNAWIADOMOSC** 14 liter

2

Każdą litera tekstu jawnego szyfrujemy korzystając z alfabetu w macierzy zaczynającego się odpowiadającą literą w haśle.

Litery tekstu jawnego

Litery klucza

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 | A |
| C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | 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 |

**DLDPZGTUFNWZME**

# Kryptografia klasyczna w Simple Cryptography

The screenshot shows the 'Simple Cryptography' web application interface. The title bar reads 'Simple Cryptography'. The main content area has a light blue background. At the top left, it says 'CRYPTOGRAPHY TOOL BY KACPER BOJANOWSKI & FILIP OPILKA'. Below this, there's a 'CHOOSE AN ACTION:' section with three buttons: 'ALGORITHMS', 'RSA', and 'SSS'. To the right, there's an 'ALGORITHMS' section with a 'CHOOSE AN ALGORITHM:' dropdown menu currently set to 'Cesar'. In the center, there's a large white text input area, an 'ENTER KEY:' label, and two buttons: 'ENCRYPT' and 'DECRYPT'. On the left side of the central area is a green vertical button labeled 'BREAK'. On the right side is a green vertical button labeled 'LETTERPLOTS'. Two white arrows point from Polish text to the interface: one from 'Łamanie szyfru Cezara' to the 'BREAK' button, and another from 'Wykresy częstotliwości liter' to the 'LETTERPLOTS' button. A third white arrow points from 'Wybór algorytmu' to the 'Cesar' dropdown menu.

CRYPTOGRAPHY TOOL  
BY KACPER BOJANOWSKI & FILIP OPILKA

CHOOSE AN ACTION:

ALGORITHMS

RSA

SSS

ALGORITHMS

CHOOSE AN ALGORITHM:

Cesar

ENTER KEY:

ENCRYPT

DECRYPT

BREAK

LETTERPLOTS

Łamanie szyfru Cezara

Wybór algorytmu

Wykresy częstotliwości liter



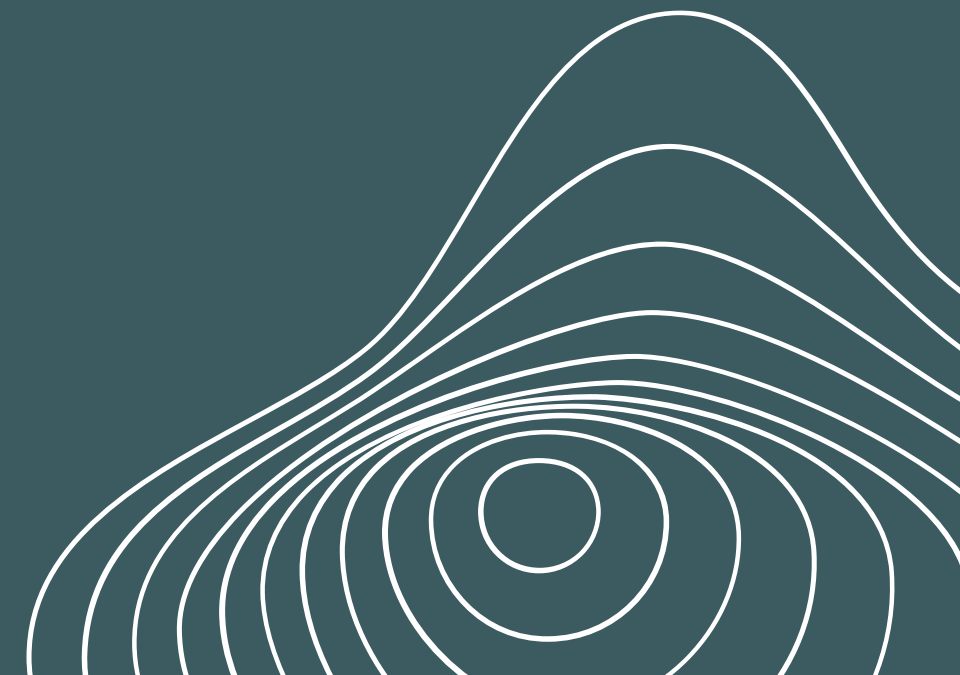
# Algorytm RSA



# Algorytm RSA

Obecnie najpopularniejszy asymetryczny algorytm kryptograficzny z kluczem publicznym.

Nazwa pochodzi od nazwisk twórców  
"Rivest-Shamir-Adleman"





# Sposób działania algorytmu

- 1 Wygenerowanie kluczy
- 2 Dystrybucja klucza
- 3 Szyfrowanie
- 4 Rozszyfrowanie

$$C = M^e \bmod n$$

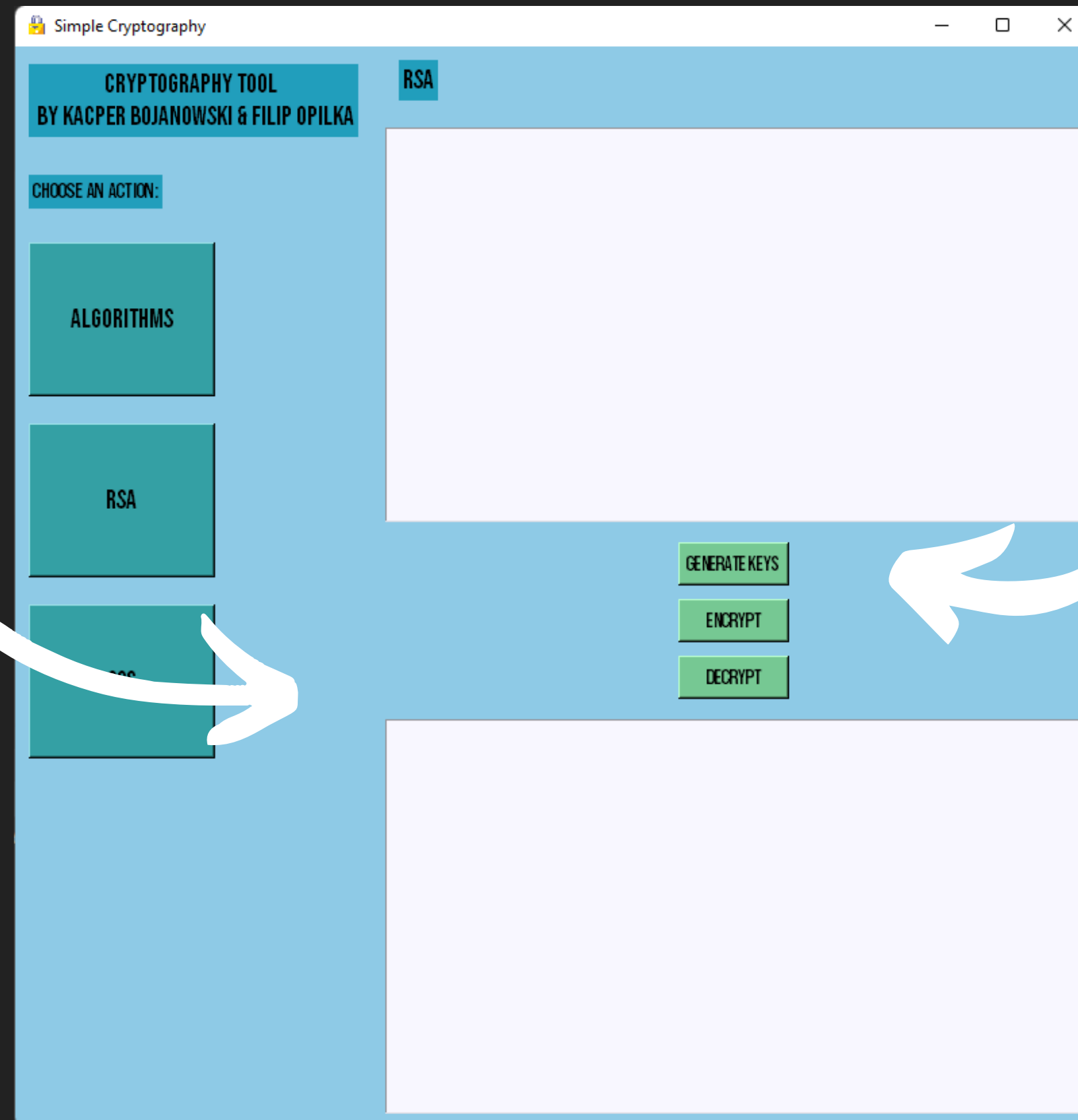
gdzie  $(e, n)$  to klucz publiczny

$$M = C^d \bmod n$$

gdzie  $(d)$  to klucz prywatny

# RSA w Simple Cryptography

Szyfrowanie i  
deszyfrowanie



Generator pary  
kluczy



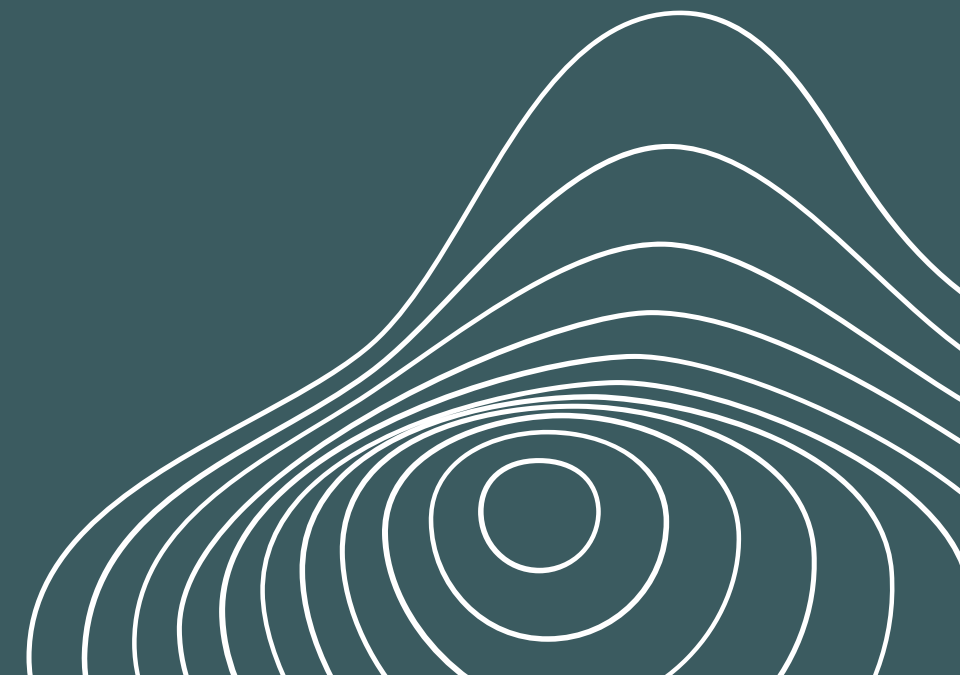
# Shamir's Secret Sharing



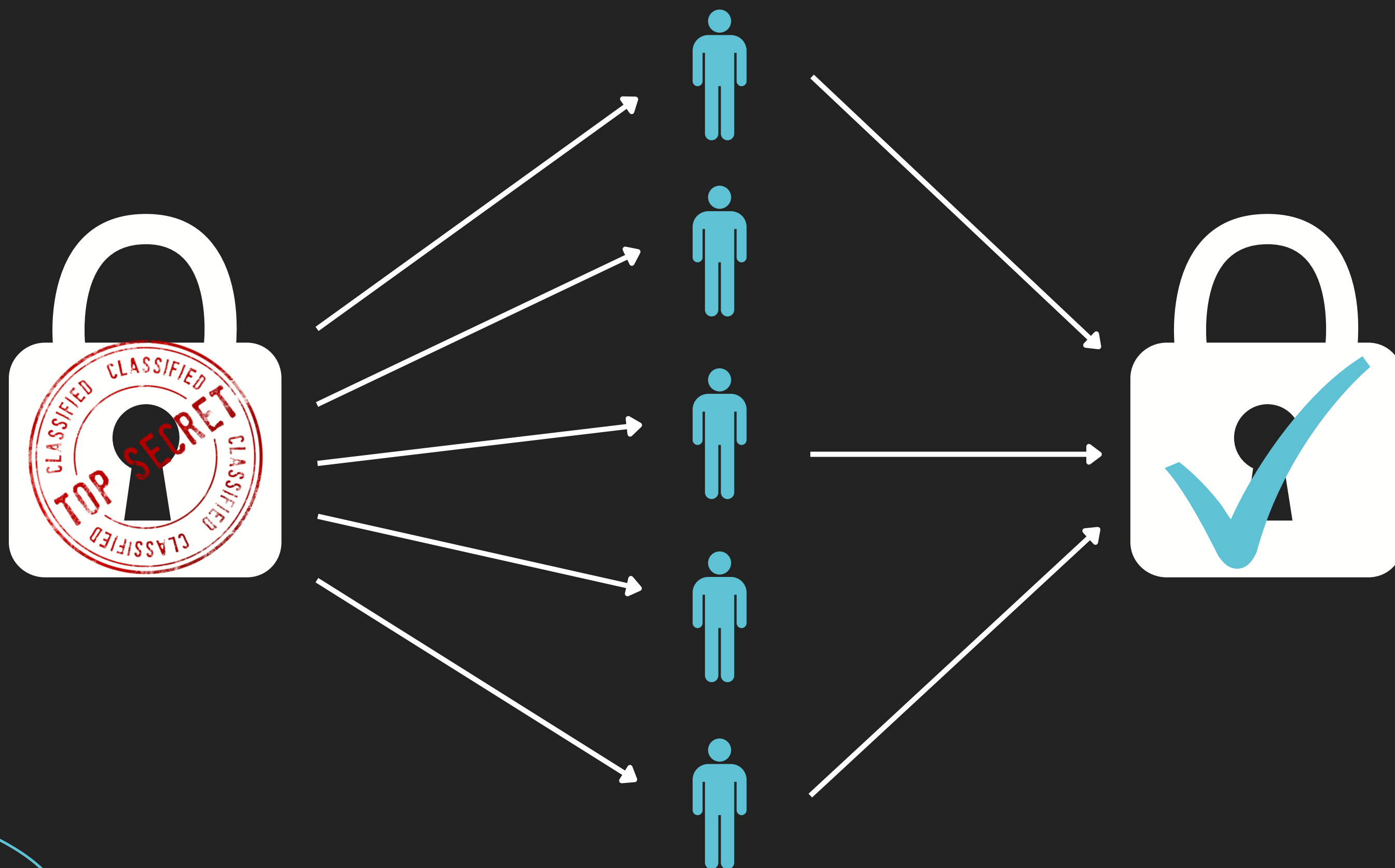
# Shamir's Secret Sharing

Jeden z pierwszych algorytmów  
umożliwiający podział sekretu. Umożliwia  
odtworzenie wiadomości na podstawie  
dowolnych "k" spośród "n" części.

Autorem jest Adi Shamir, współtwórca  
algorytmu RSA.



# Zasada działania



# Sposób szyfrowania

1 Sekret: 1234

2  $n = 5$        $k = 3$

3  $f(x) = 94x^2 + 166x + 1234$

$$ax^2 + bx + c = 0$$

4

$P1 = (1, 1494)$

$P2 = (2, 1942)$

$P3 = (3, 2578)$

$P4 = (4, 3402)$

$P5 = (5, 4414)$



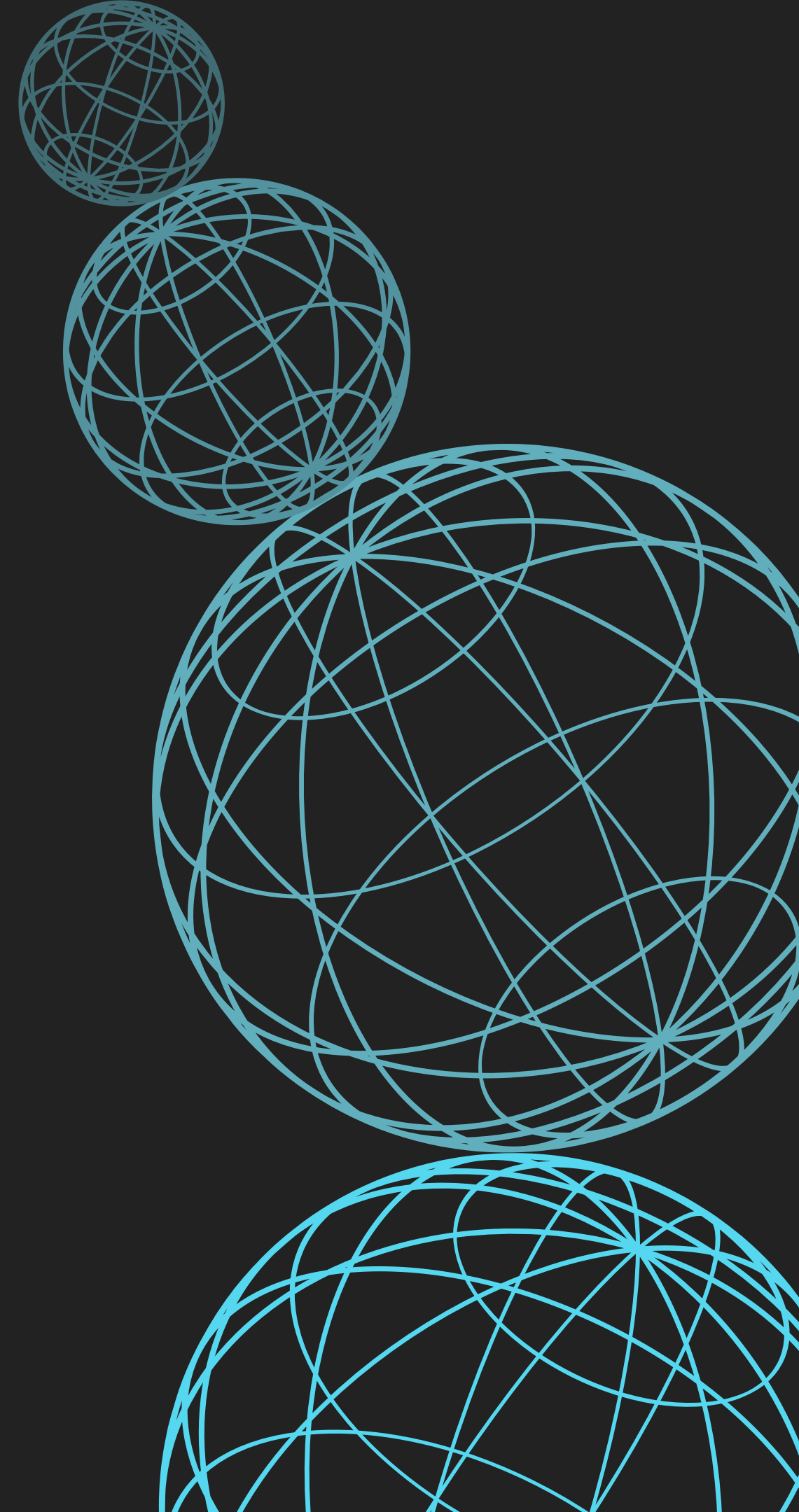
5

Rekonstrukcja



# Dziękujemy!

Macie jakieś pytania?





# Bibliografia



- [https://pl.wikipedia.org/wiki/Szyfr\\_Playfair](https://pl.wikipedia.org/wiki/Szyfr_Playfair)
- <https://mattomatti.com/pl/a35ag>
- [https://en.wikipedia.org/wiki/Shamir%27s\\_Secret\\_Sharing](https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing)
- <https://apogiatzis.medium.com/shamirs-secret-sharing-a-numeric-example-walkthrough-a59b288c34c4>
- [https://en.wikipedia.org/wiki/Adi\\_Shamir](https://en.wikipedia.org/wiki/Adi_Shamir)
- <https://www.geeksforgeeks.org/implementing-shamirs-secret-sharing-scheme-in-python>
- <http://practicalcryptography.com/ciphers/>
- [https://www.youtube.com/watch?v=vf1z7GIG6Qo&t=272s&ab\\_channel=Simplilearn](https://www.youtube.com/watch?v=vf1z7GIG6Qo&t=272s&ab_channel=Simplilearn)