# Kryptografia jest wśród nas

Maciej Grześkowiak

Uniwersytet im. Adama Mickiewicza w Poznaniu
Wydział Matematyki i Informatyki

KOALA
Drużynowy konkurs matematyczno-informatyczny
Poznań, 3 lutego 2018 roku

# Gdzie jest kryptografia?

# Gdzie jest kryptografia?

# Gdzie jest kryptografia?

# Gdzie jest kryptografia?

# Gdzie jest kryptografia?

# Gdzie jest kryptografia?

# Gdzie jest kryptografia?

# Co to jest kryptografia?

KRYPTOLOGIA

# Co to jest kryptografia?

KRYPTOLOGIA

KRYPTOGRAFIA

# Co to jest kryptografia?

KRYPTOLOGIA

KRYPTOGRAFIA

KRYPTOANALIZA

# Co to jest kryptografia?

KRYPTOLOGIA

KRYPTOGRAFIA

Projektowanie:

Protokoły

Algorytmy

KRYPTOANALIZA

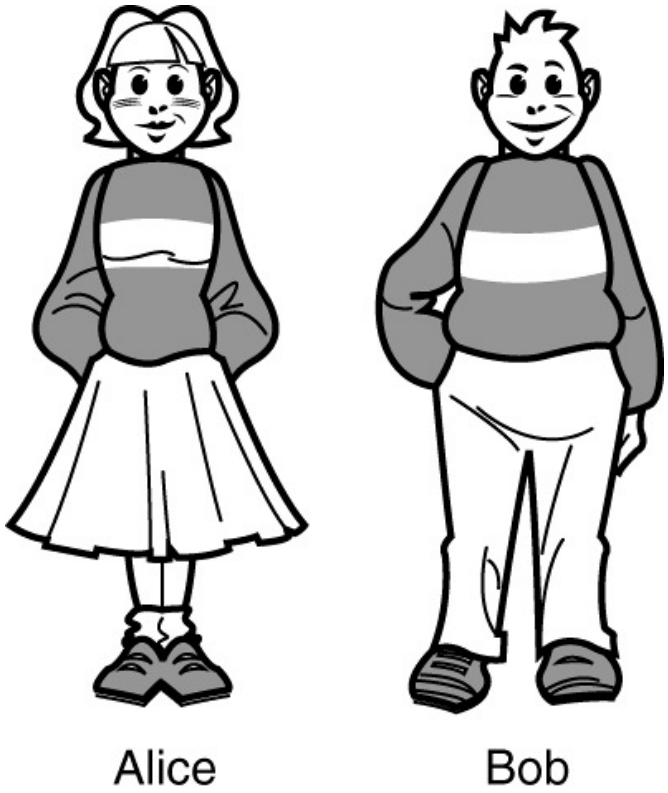
# Co to jest kryptografia?

KRYPTOLOGIA

KRYPTOGRAFIA
Projektowanie:
Protokoły
Algorytmy

KRYPTOANALIZA
Łamanie:
Protokoły
Algorytmy

# Uczestnicy protokołu: Alice i Bob



# Uczestnicy protokołu: Mallet

# Kryptografia może zapewnić poufność

# Symetryczny Protokół Szyfrowania

ALICE,

# Symetryczny Protokół Szyfrowania

ALICE, BOB

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$
2. Uzgadniają w bezpieczny sposób $K$

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$
2. Uzgadniają w bezpieczny sposób $K$
3. Alice tworzy $M$

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$
2. Uzgadniają w bezpieczny sposób $K$
3. Alice tworzy $M$
4. Alice oblicza $E_K(M) = C$

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$
2. Uzgadniają w bezpieczny sposób $K$
3. Alice tworzy $M$
4. Alice oblicza $E_K(M) = C$
5. Alice wysyła do Boba $C$

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$
2. Uzgadniają w bezpieczny sposób $K$
3. Alice tworzy $M$
4. Alice oblicza $E_K(M) = C$
5. Alice wysyła do Boba $C$
6. Bob oblicza $D_K(C) = M$

# Symetryczny Protokół Szyfrowania

ALICE, BOB

1. Uzgadniają jawnie $(E, D)$
2. Uzgadniają w bezpieczny sposób $K$
3. Alice tworzy $M$
4. Alice oblicza $E_K(M) = C$
5. Alice wysyła do Boba $C$
6. Bob oblicza $D_K(C) = M$

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$0 \quad XOR \quad 1 = 1, \qquad 1 \quad XOR \quad 1 = 0$$

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$0 \quad XOR \quad 1 = 1, \qquad 1 \quad XOR \quad 1 = 0$$

$$0010 \quad XOR \quad 1100 = 1110, \qquad 1101 \quad XOR \quad 0101 = 1000$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$M = \quad 01000001$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$M = \quad 01000001 \quad 01001100$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$M = \quad 01000001 \quad 01001100 \quad 01000001$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$M = \quad 01000001 \quad 01001100 \quad 01000001$$
$$K = \quad 01101010 \quad 11001101 \quad 01010010$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$
\begin{aligned}
M &= \quad 01000001 \quad 01001100 \quad 01000001 \\
K &= \quad 01101010 \quad 11001101 \quad 01010010 \\
C &= \quad 00101011
\end{aligned}
$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$
\begin{aligned}
M &= \quad 01000001 \quad 01001100 \quad 01000001 \\
K &= \quad 01101010 \quad 11001101 \quad 01010010 \\
C &= \quad 00101011 \quad 10000001
\end{aligned}
$$

# Szyfrowanie XOR

Metoda szyfrowania $E$

1. Ustal wiadomość $M = ALA$
2. Wylosuj klucz tajny $K$. Klucz $K$ bezpiecznie prześlij do Boba
3. Oblicz $C = M \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$
\begin{aligned}
M = &\quad 01000001 \quad 01001100 \quad 01000001 \\
K = &\quad 01101010 \quad 11001101 \quad 01010010 \\
C = &\quad 00101011 \quad 10000001 \quad 01010011
\end{aligned}
$$

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$
3. Oblicz $M = C \quad XOR \quad K$

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$
3. Oblicz $M = C \quad XOR \quad K$
4. Wyślij $C$ do Boba

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$
3. Oblicz $M = C \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$K = \quad 01101010 \quad 11001101 \quad 01010010$$

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$
3. Oblicz $M = C \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$K = \quad 01101010 \quad 11001101 \quad 01010010$$
$$C = \quad 00101011 \quad 10000001 \quad 01010011$$

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$
3. Oblicz $M = C \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$
\begin{aligned}
K &= \quad 01101010 \quad 11001101 \quad 01010010 \\
C &= \quad 00101011 \quad 10000001 \quad 01010011 \\
M &= \quad 01000001 \quad 01001100 \quad 01000001
\end{aligned}
$$

# Deszyfrowanie XOR

Metoda deszyfrowania $D$

1. Pobierz klucz tajny $K$.
2. Pobierz szyfrogram $C$
3. Oblicz $M = C \quad XOR \quad K$
4. Wyślij $C$ do Boba

$$
\begin{aligned}
K &= \quad 01101010 \quad 11001101 \quad 01010010 \\
C &= \quad 00101011 \quad 10000001 \quad 01010011 \\
M &= \quad 01000001 \quad 01001100 \quad 01000001
\end{aligned}
$$

$$M = ALA$$

# Wady i zalety szyfrowania XOR

1. Załóżmy, że klucz $K$ jest wybrany w sposób losowy,

$$K = b_1 b_2 \ldots b_j \ldots b_s$$

# Wady i zalety szyfrowania XOR

1. Załóżmy, że klucz $K$ jest wybrany w sposób losowy,

$$K = b_1 b_2 \dots b_j \dots b_s$$

2. Ustalmy wiadomość

$$M = m_1 m_2 \dots m_j \dots m_s$$

# Wady i zalety szyfrowania XOR

1. Załóżmy, że klucz $K$ jest wybrany w sposób losowy,

$$K = b_1 b_2 \dots b_j \dots b_s$$

2. Ustalmy wiadomość

$$M = m_1 m_2 \dots m_j \dots m_s$$

3. Wtedy szyfrogram $C = M \quad XOR \quad K$

$$C = c_1 c_2 \dots c_j \dots c_s$$

# Wady i zalety szyfrowania XOR

1. Załóżmy, że klucz $K$ jest wybrany w sposób losowy,

$$K = b_1 b_2 \ldots b_j \ldots b_s$$

2. Ustalmy wiadomość

$$M = m_1 m_2 \ldots m_j \ldots m_s$$

3. Wtedy szyfrogram $C = M \quad XOR \quad K$

$$C = c_1 c_2 \ldots c_j \ldots c_s$$

4. Jakie jest prawdopodobieństwo tego, że $c_j = 0$?

# Wady i zalety szyfrowania XOR

1. Załóżmy, że klucz $K$ jest wybrany w sposób losowy,

$$K = b_1 b_2 \ldots b_j \ldots b_s$$

2. Ustalmy wiadomość

$$M = m_1 m_2 \ldots m_j \ldots m_s$$

3. Wtedy szyfrogram $C = M \quad XOR \quad K$

$$C = c_1 c_2 \ldots c_j \ldots c_s$$

4. Jakie jest prawdopodobieństwo tego, że $c_j = 0$?

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$c_j = m_j \quad XOR \quad k_j, \qquad c_j = 0?$$

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$c_j = m_j \quad XOR \quad k_j, \qquad c_j = 0?$$

WADA:

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$c_j = m_j \quad XOR \quad k_j, \qquad c_j = 0?$$

WADA: Klucz $K$ musi być tej samej długości co wiadomość $M$

# Operacja XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$c_j = m_j \quad XOR \quad k_j, \qquad c_j = 0?$$

WADA: Klucz $K$ musi być tej samej długości co wiadomość $M$

ZALETA:

# Operacja XOR

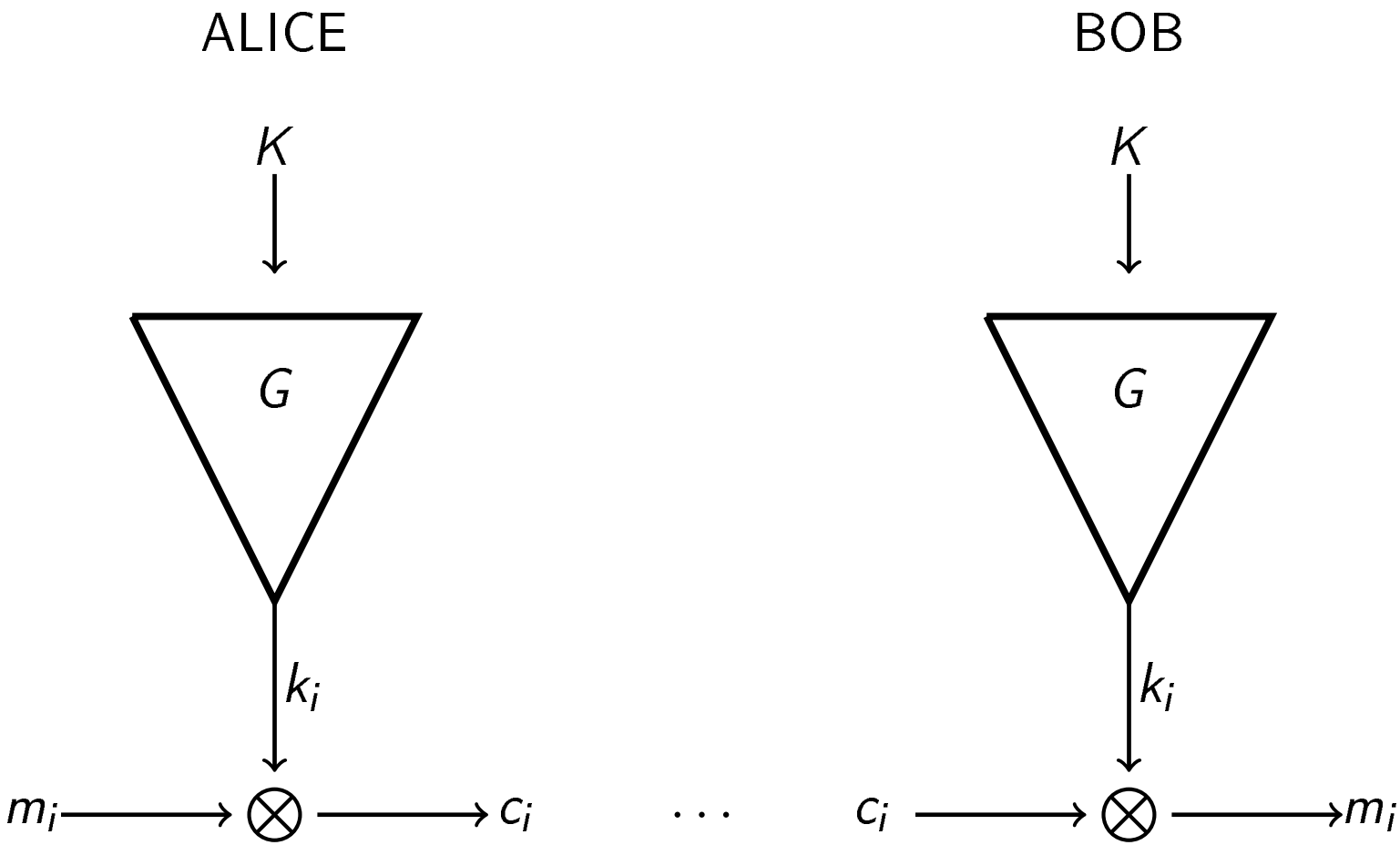
| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$$c_j = m_j \quad XOR \quad k_j, \qquad c_j = 0?$$

WADA: Klucz $K$ musi być tej samej długości co wiadomość $M$

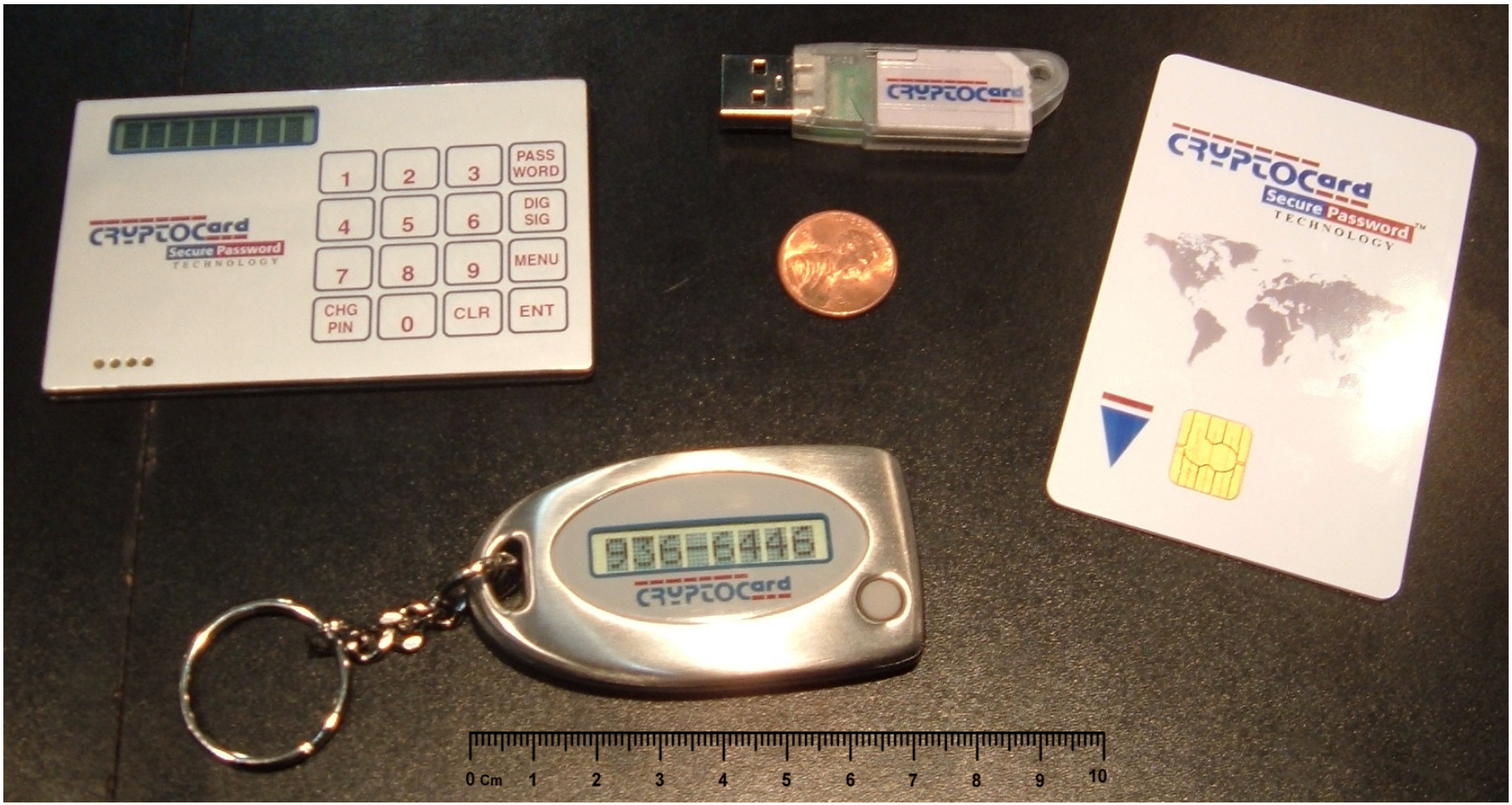
ZALETA: Bezpieczeństwo doskonałe!

# Szyfrowanie strumieniowe

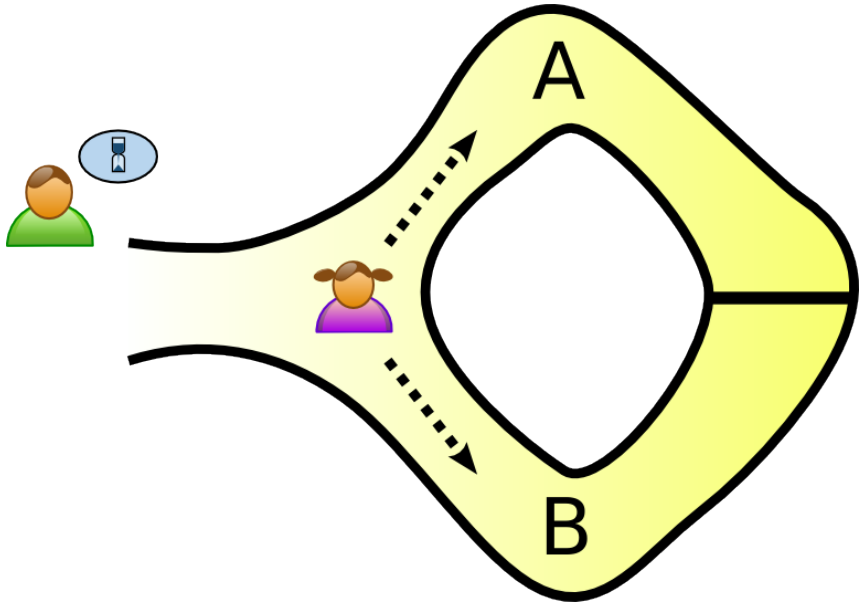


# Kryptografia może uwierzytelniać

# Narzędzia do uwierzytelniania



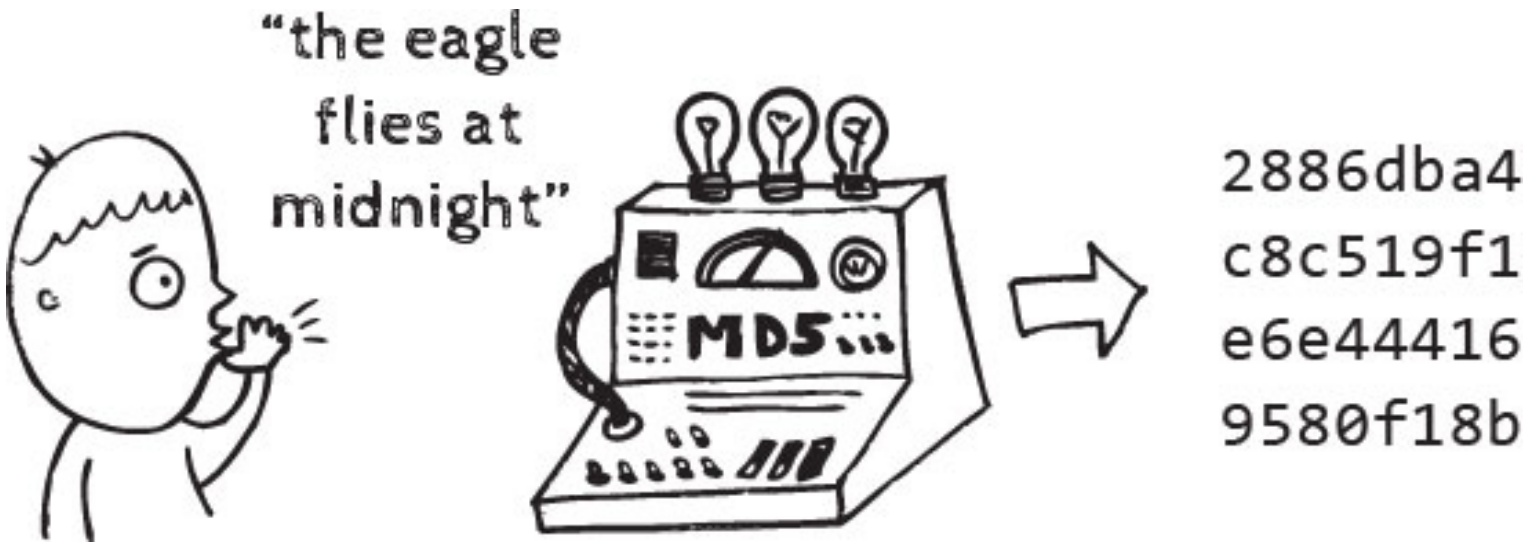
# Uwierzytelnienie



# Funkcje hashujące

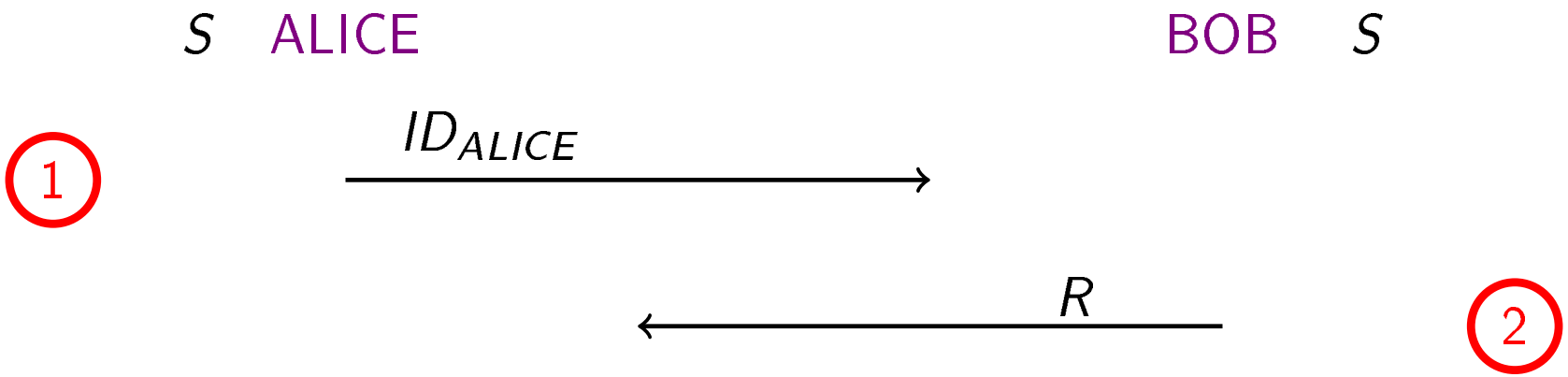
# Funkcje hashujące

# Funkcje hashujące

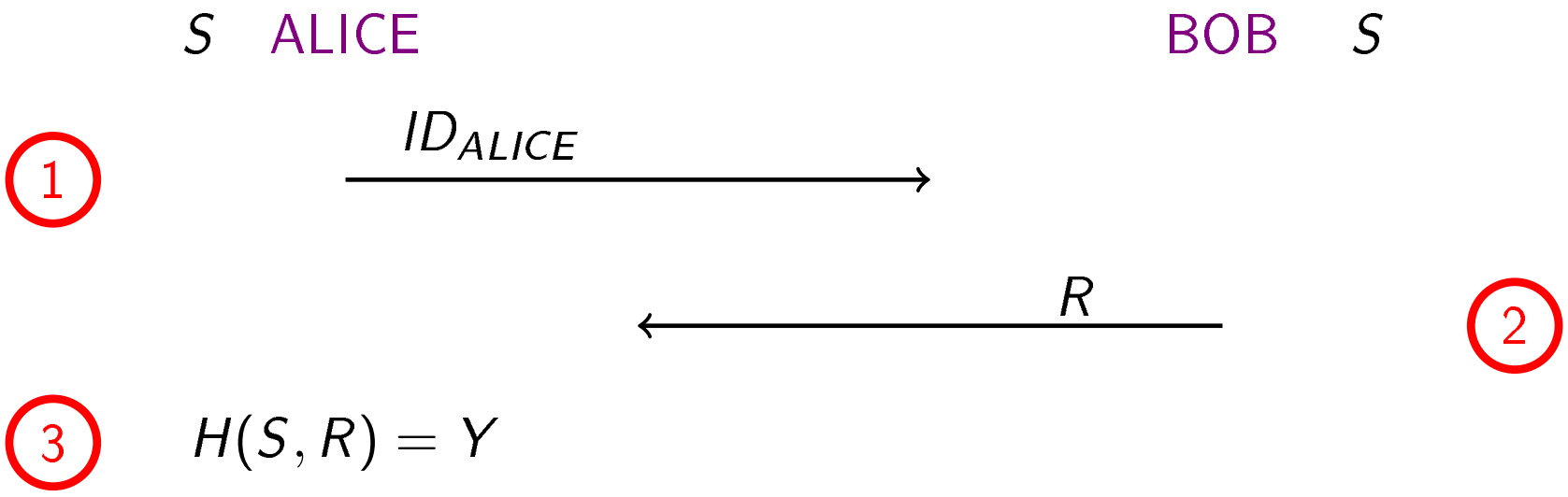


# Uwierzytelnienie, Challenge and response

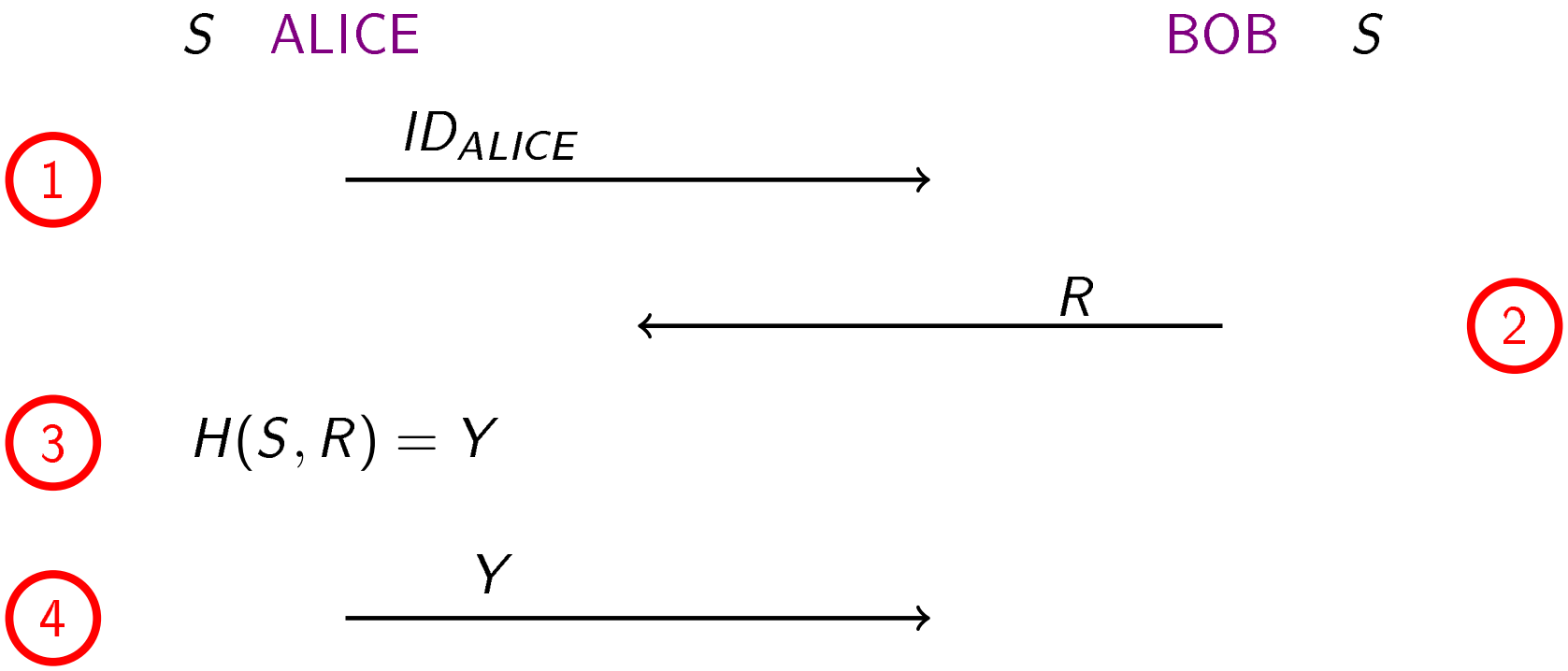
# Uwierzytelnienie, Challenge and response



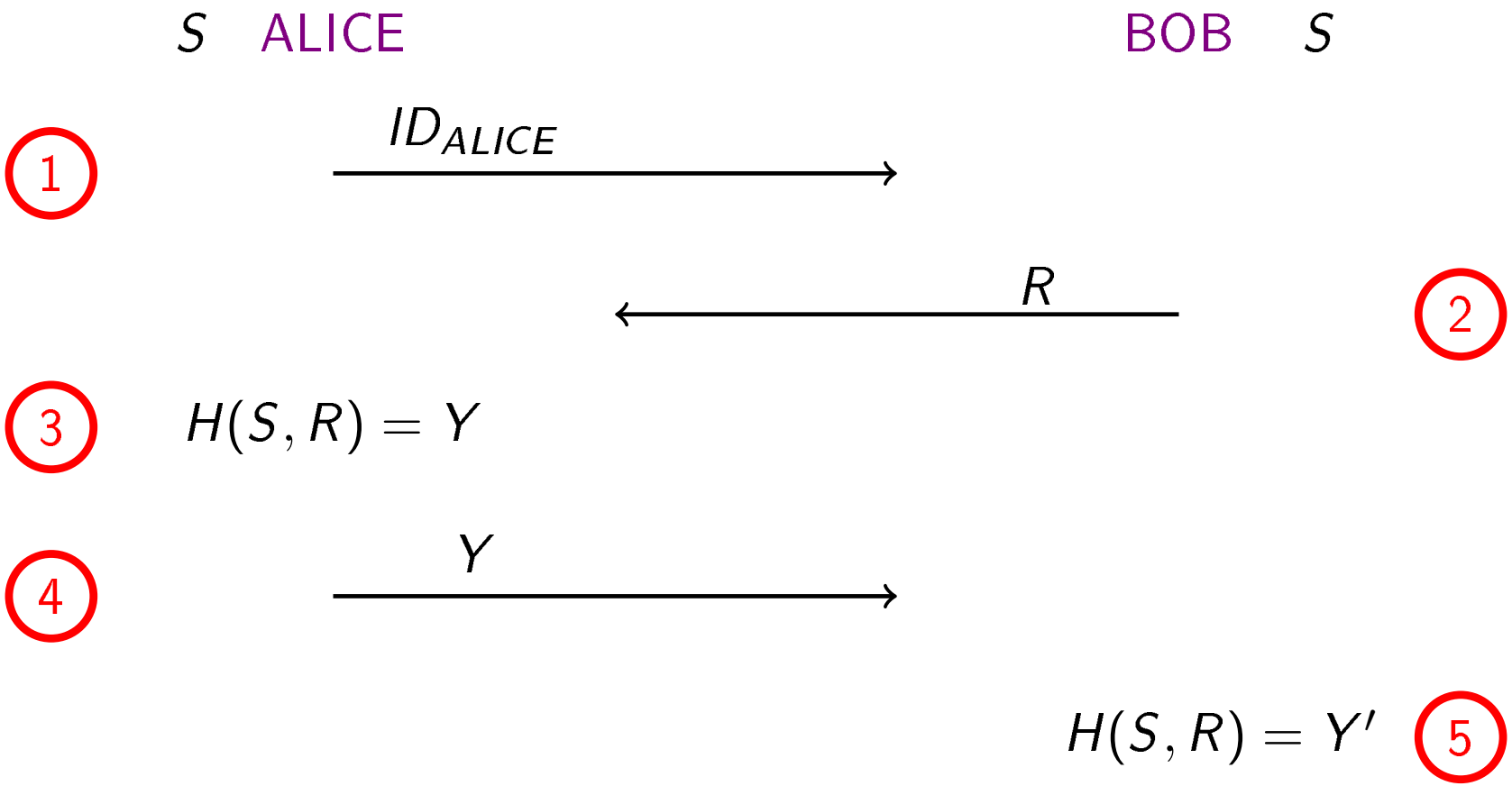
# Uwierzytelnienie, Challenge and response



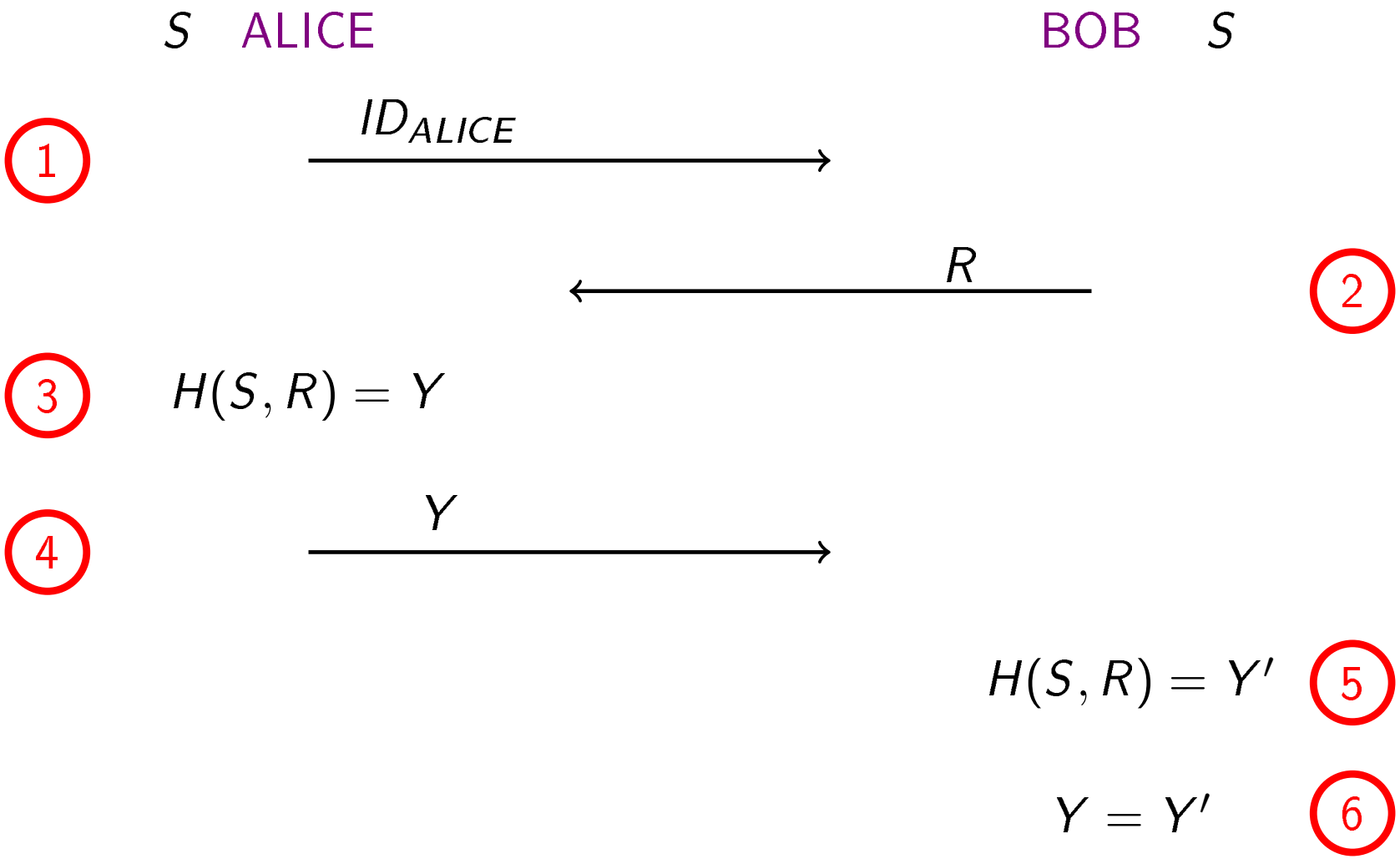
# Uwierzytelnienie, Challenge and response



# Uwierzytelnienie, Challenge and response



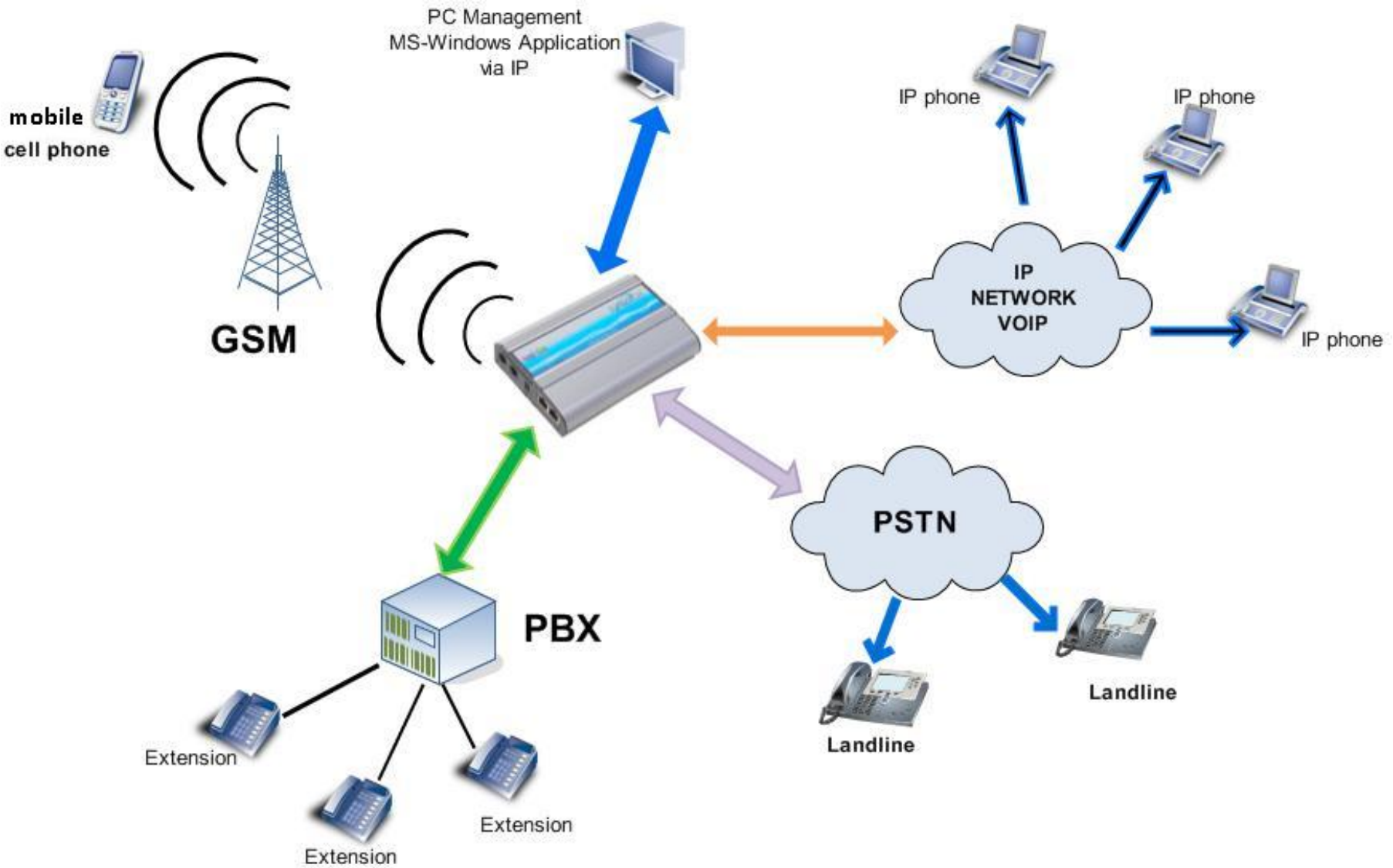
# Uwierzytelnienie, Challenge and response



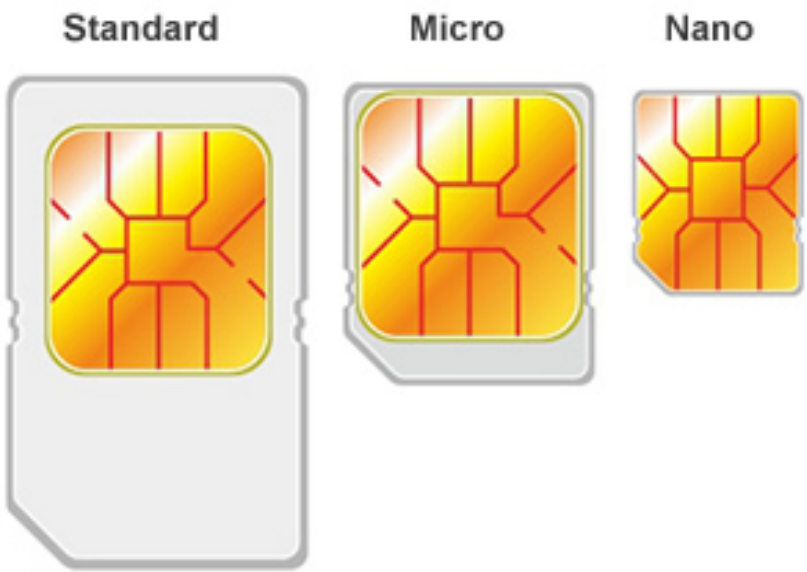
# Praktyka


SAMSUNG
14:47
Tue, 5 Mar
Tap to add city
Google
Phone
Contacts
Messaging
Internet
Apps
ChatON
Camera
Samsung Apps
Play Store

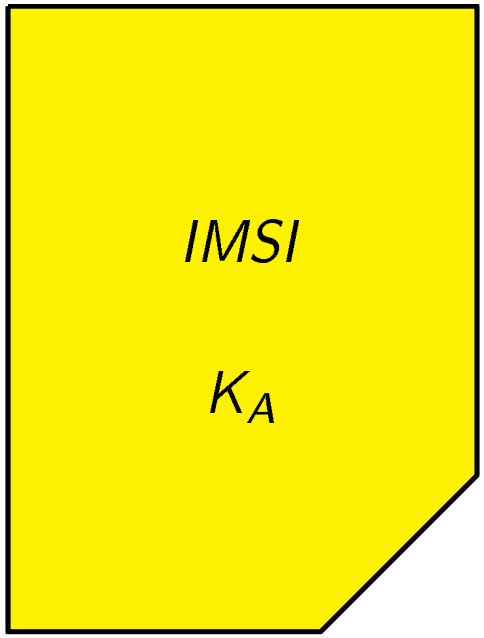
# Funkcje hashujące



# Karta SIM



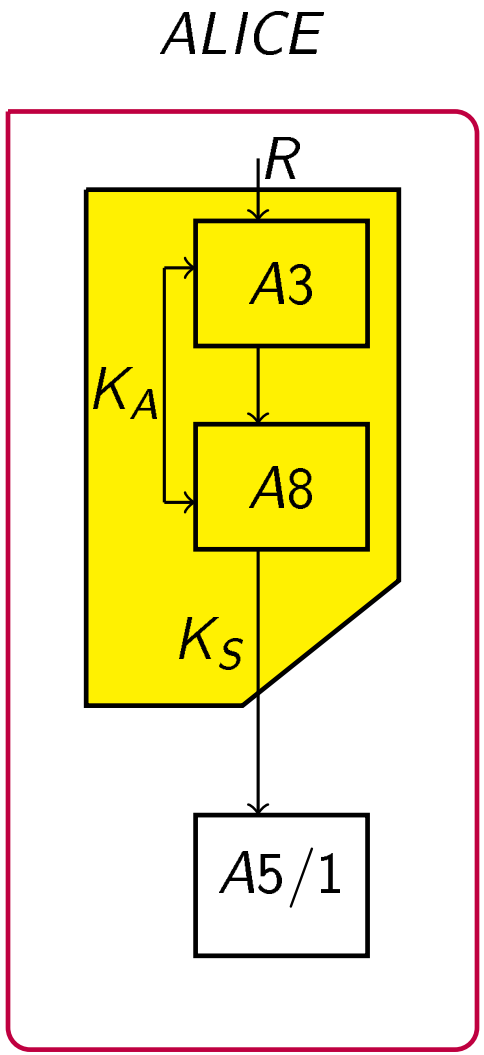
# Co zawiera SIM?



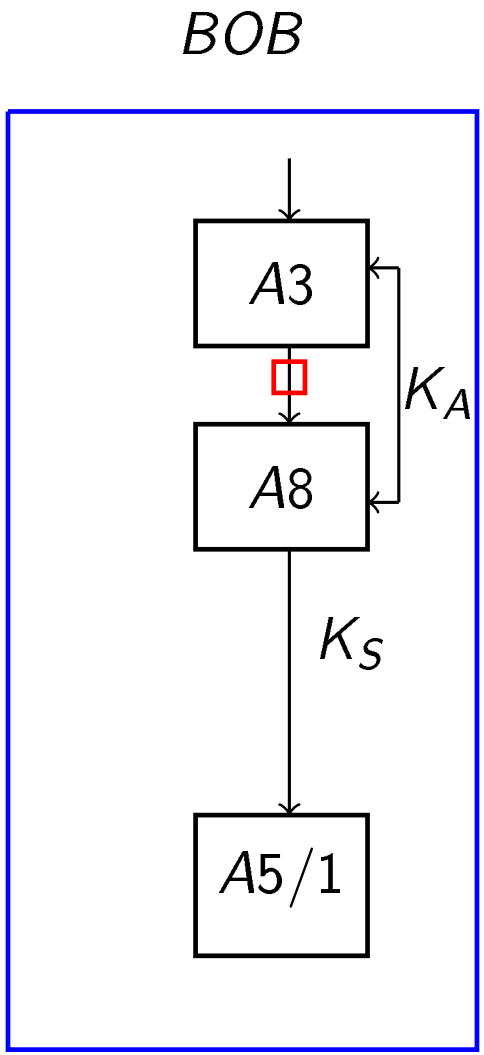

$$IMSI = International \;\; Mobile \;\; Subscriber \;\; Identity$$

$$K_A = losowy, \;\; 128 - bitowy \;\; klucz \;\; Alice$$

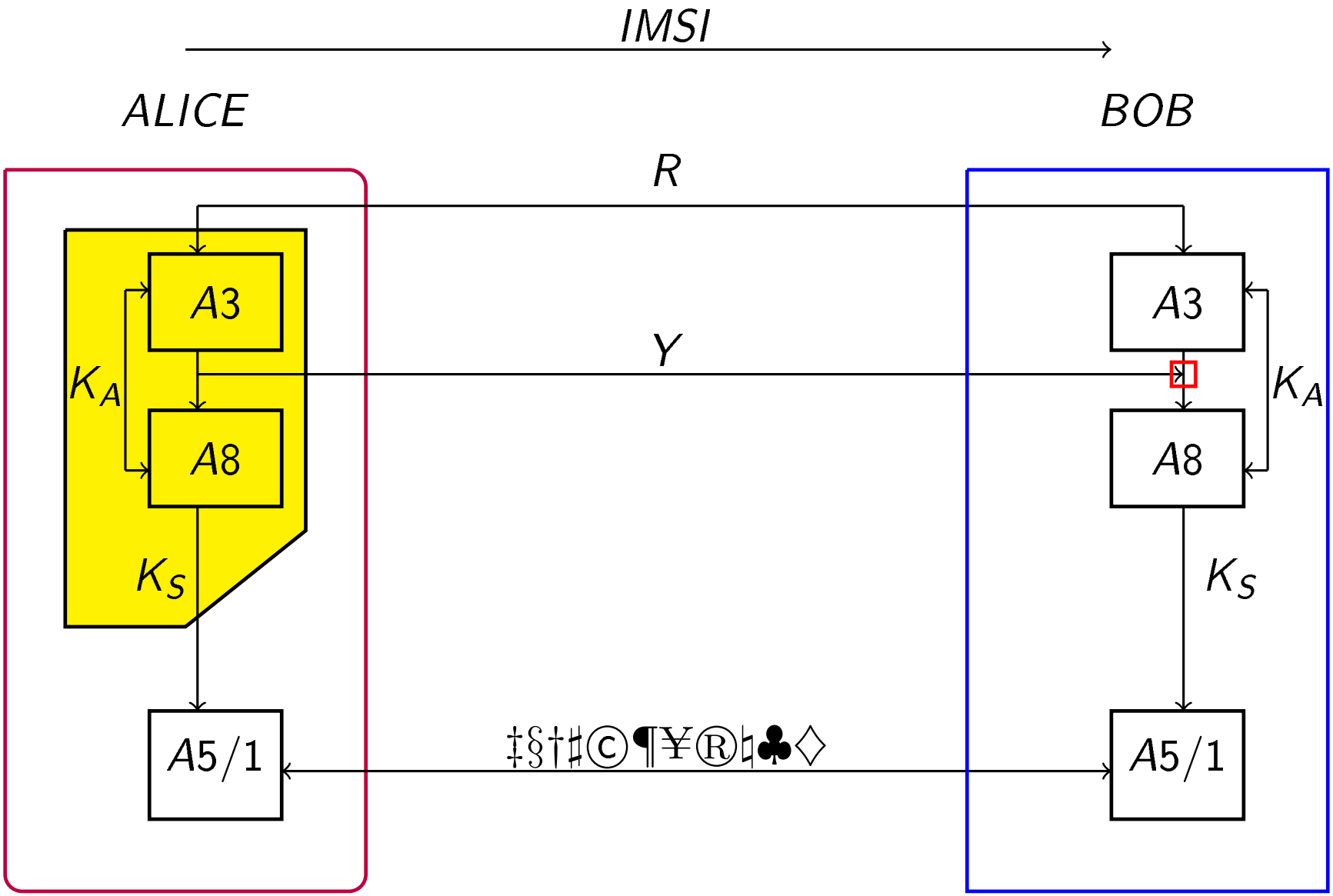
# Co zawiera telefon?



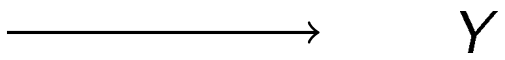
# Centrum uwierzytalniające telefonu



# Uwierzytelnienie, poufność, anonimowość



# Uwierzytelnienie Alice



# Uwierzytelnienie Alice

$$\longrightarrow \qquad Y$$

$$A3(R, K_A) = Y'$$

# Uwierzytelnienie Alice

$$\longrightarrow \qquad Y$$

$$A3(R, K_A) = Y'$$

$$Y = Y'$$