Kryptografia

z elementami kryptografii kwantowej

Ryszard Tanaś

http://zon8.physd.amu.edu.pl/~tanas

Wykład 1

Spis treści

1 Kryptografia klasyczna — wstęp **4**

1.1 Literatura 4

1.2 Terminologia 6

1.3 Główne postacie 7

1.4 Kanał łączności 8

2 Proste szyfry **10**

2.1 Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny 10

2.2 Szyfr Vigenère'a 11

2.3 Szyfr Vernama (one-time pad) 12

3 Współczesne kryptosystemy **13**

3.1 Systemy z kluczem tajnym 13

3.2 Systemy z kluczem publicznym 15

4 Kryptografia bardziej formalnie 20

4.1 Szyfrowanie i deszyfrowanie 20
4.2 Algorytmy 21
4.3 Przykład kryptogramu 22
4.4 Podstawowe zastosowania 23
4.5 Jak to działa: algorytm symetryczny 24
4.6 Jak to działa: algorytm asymetryczny 26
4.7 Kryptosystem hybrydowy 28
4.8 Podpis cyfrowy: kryptosystem z kluczem publicznym 30
4.9 Jednokierunkowe funkcje hashujące (skrótu) 32
4.10 Elektroniczny notariusz 33
4.11 Operacja XOR i szyfr Vernama 34

1 Kryptografia klasyczna — wstęp

1.1 Literatura

- M. Kutyłowski i W. B. Strothmann Kryptografia: Teoria i praktyka zabezpieczania systemów komputerowych, Wyd. READ ME, Warszawa, 1999, drugie wydanie dostępne w księgarniach
- B. Schneier Kryptografia dla praktyków, WNT, Warszawa, 2002, wydanie drugie
- D. R. Stinson, Kryptografia,WNT, Warszawa, 2005
- R. Wobst, Kryptologia. Budowa i łamanie zabezpieczeń, RM, Warszawa, 2002

- A. J. Menezes, P. C. van Oorschot, S. A. Vanstone Kryptografia stosowana, WNT W-wa, 2005
  Handbook of Applied Cryptography, CRC Press, 1997, New York, dostępna w Internecie
- S. J. Lomonaco A quick glance at quantum cryptography, LANL quant-ph archive, quant-ph/9811056, 1998
- S. J. Lomonaco A talk on quantum cryptography or how Alice outwits Eve, LANL quantum-ph archive, quant-ph/0102016, 2001
- N. Gisin, G. Ribordy, W. Titel, H. Zbinden Quantum cryptography, LANL quant-ph archive, quant-ph/0101098, 2001

1.2 Terminologia

- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)
- Kryptoanaliza — łamanie szyfrów
- Kryptologia — dział matematyki, który zajmuje się podstawami metod kryptograficznych (kryptografia + kryptoanaliza)

1.2 Terminologia

- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)
- Kryptoanaliza — łamanie szyfrów
- Kryptologia — dział matematyki, który zajmuje się podstawami metod kryptograficznych (kryptografia + kryptoanaliza)

1.2 Terminologia

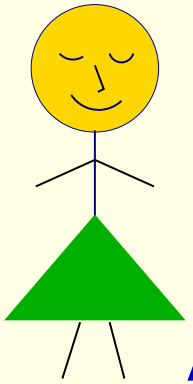
- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)
- Kryptoanaliza — łamanie szyfrów
- Kryptologia — dział matematyki, który zajmuje się podstawami metod kryptograficznych (kryptografia + kryptoanaliza)

1.2 Terminologia

- Kryptografia — dziedzina wiedzy zajmująca się zabezpieczaniem informacji (szyfrowanie)
- Kryptoanaliza — łamanie szyfrów
- Kryptologia — dział matematyki, który zajmuje się podstawami metod kryptograficznych (kryptografia + kryptoanaliza)

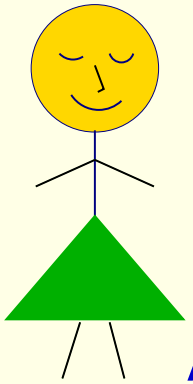
1.3 Główne postacie

1.3 Główne postacie

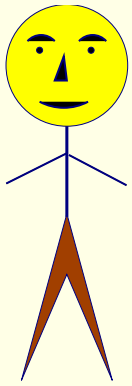


Alicja — nadawca informacji

1.3 Główne postacie

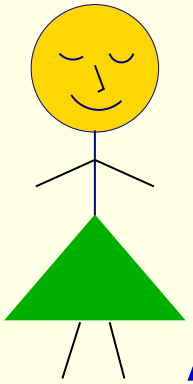


Alicja — nadawca informacji

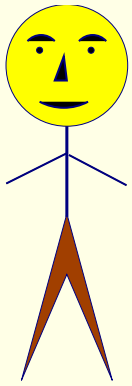


Bolek — odbiorca (adresat) informacji

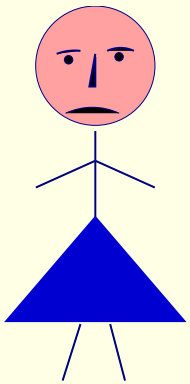
1.3 Główne postacie



Alicja — nadawca informacji

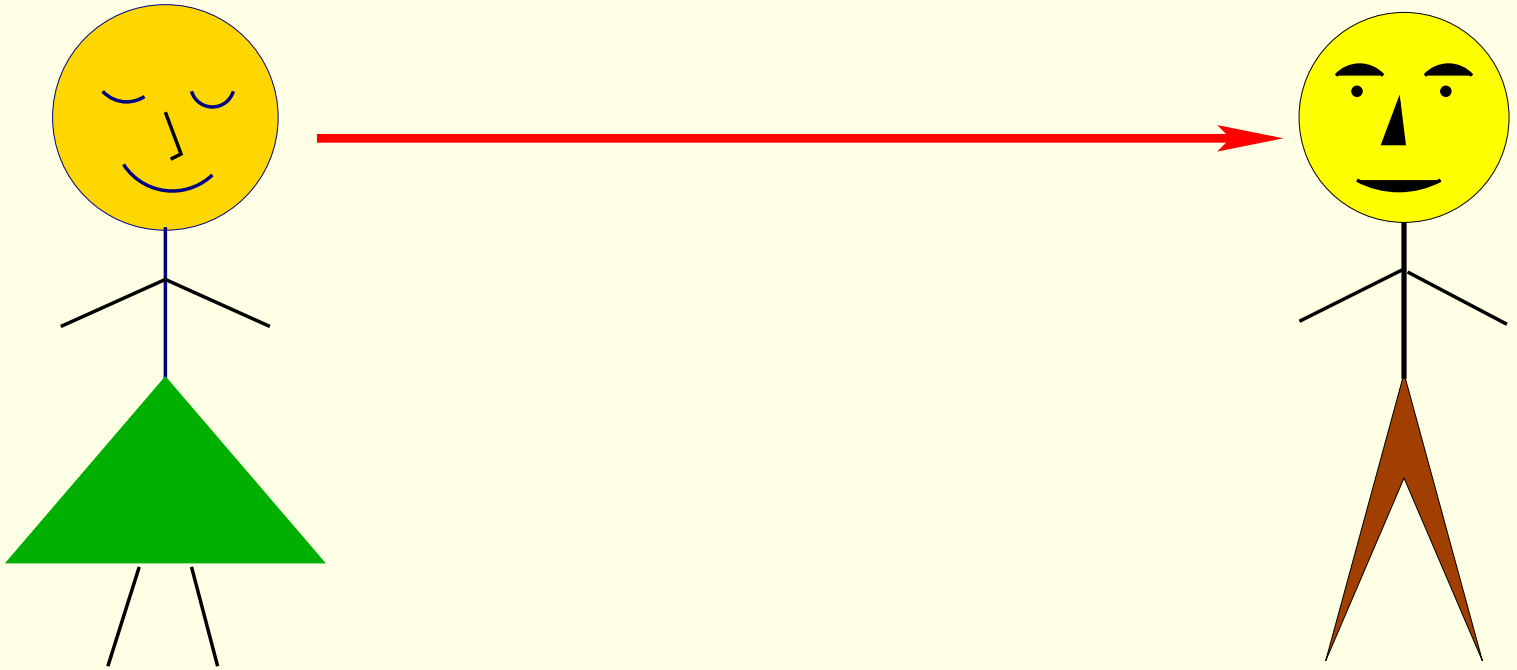


Bolek — odbiorca (adresat) informacji

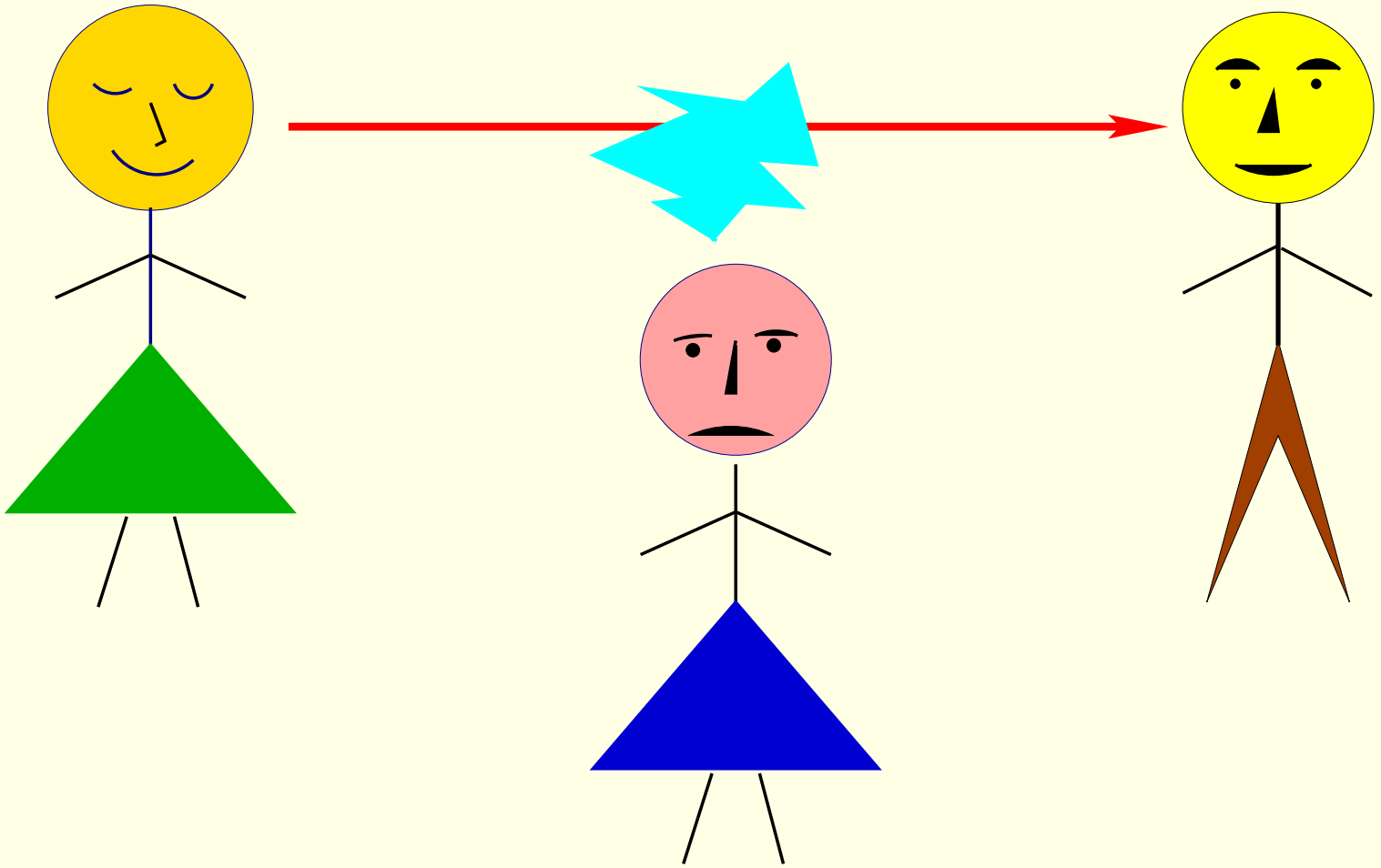


Ewa — usiłująca przechwycić informację przeznaczoną dla Bolka

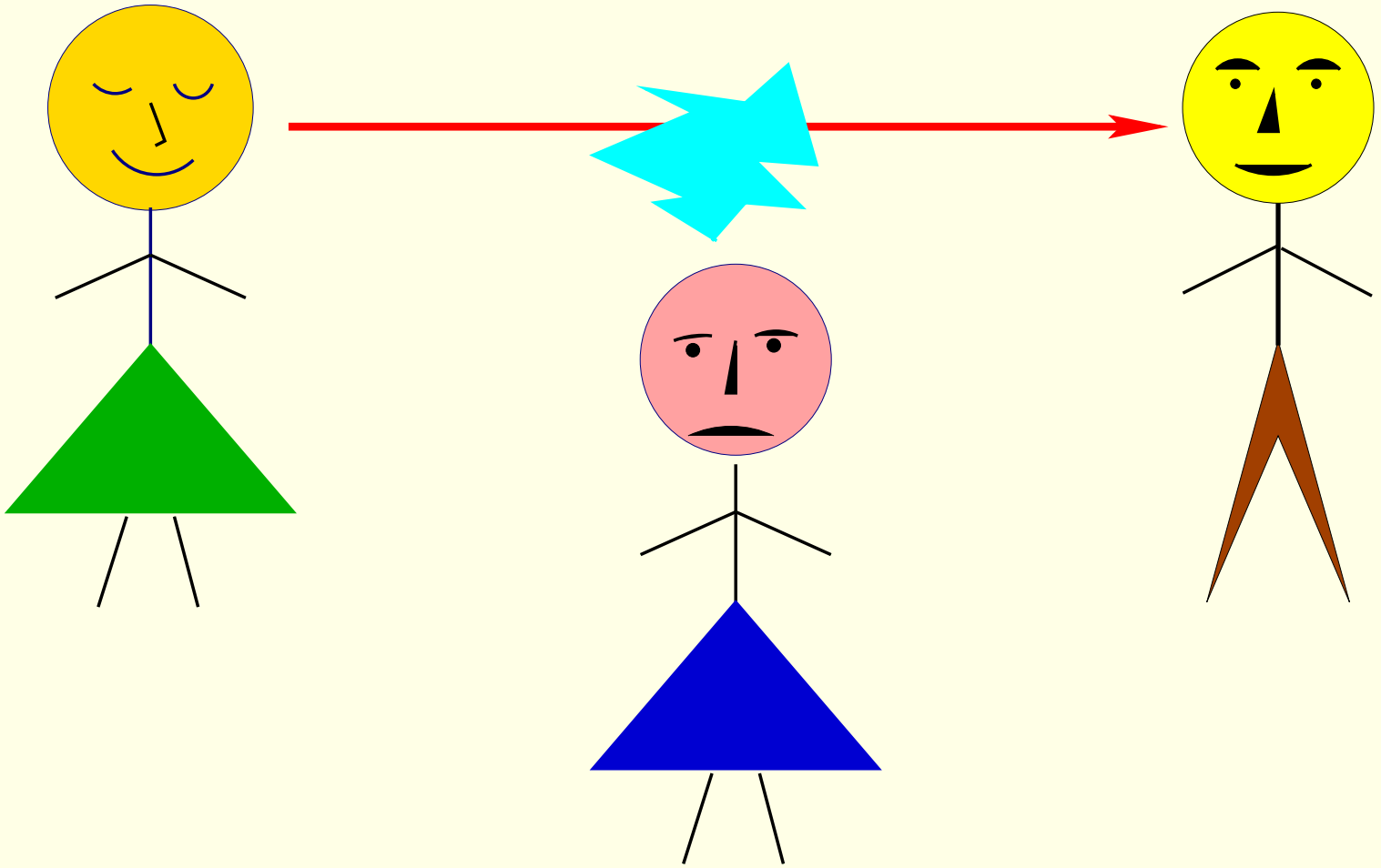
1.4 Kanał łączności



Alicja przesyła informacje do Bolka kanałem, który jest narażony na podsłuch

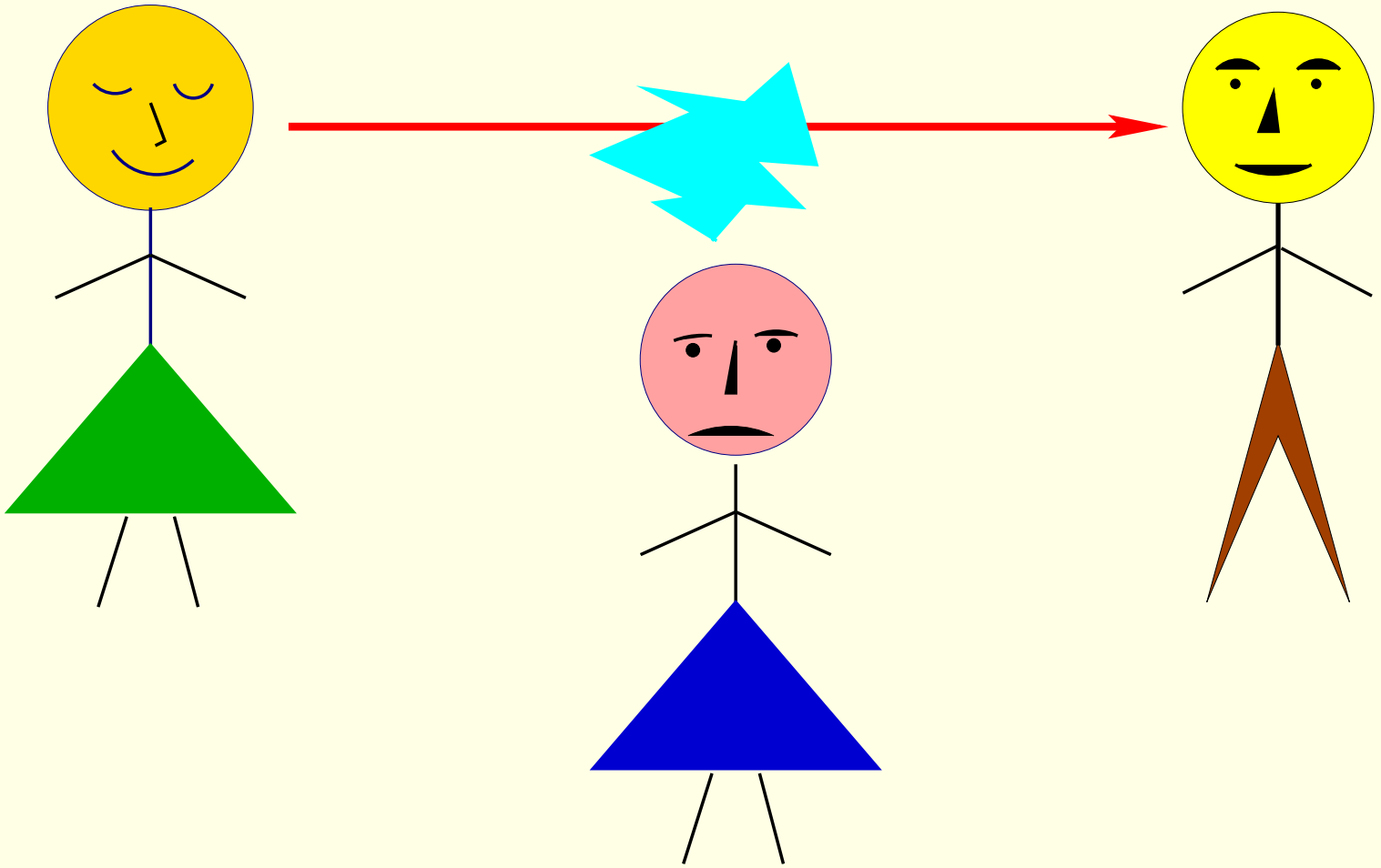


Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka



Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka

Co powinna zrobić Alicja?



Ewa podsłuchuje usiłując dowiedzieć się co Alicja przesyła do Bolka

Co powinna zrobić Alicja?

Szyfrować!

2 Proste szyfry

2.1 Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

2 Proste szyfry

2.1 Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

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
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

2 Proste szyfry

2.1 Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

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
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

tekst jawny $\longrightarrow$ K R Y P T O G R A F I A
kryptogram $\longrightarrow$ N U B T W S J U D I L D

2.2 Szyfr Vigenère'a

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

klucz $\longrightarrow$ S Z Y M P A N S S Z Y M

tekst $\longrightarrow$ K R Y P T O G R A F I A

krypt. $\longrightarrow$ C P W C I O U I S E G M

2.3 Szyfr Vernama (one-time pad)

tekst jawny	$\longrightarrow$	S	Z	Y	F	R
binarnie	$\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz	$\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram	$\longrightarrow$	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

2.3 Szyfr Vernama (one-time pad)

tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

2.3 Szyfr Vernama (one-time pad)

tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

2.3 Szyfr Vernama (one-time pad)

tekst jawny	$\longrightarrow$	S	Z	Y	F	R
binarnie	$\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz	$\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram	$\longrightarrow$	00100001	00001111	10000101	11110101	01111001

- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

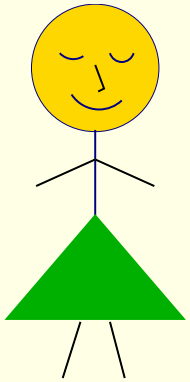
2.3 Szyfr Vernama (one-time pad)

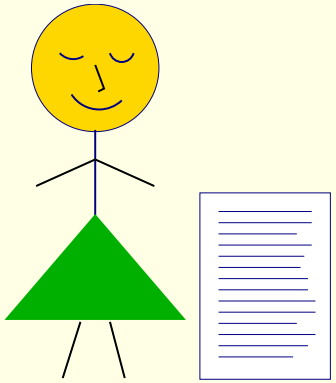
tekst jawny	$\longrightarrow$	S	Z	Y	F	R
binarnie	$\longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz	$\longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram	$\longrightarrow$	00100001	00001111	10000101	11110101	01111001

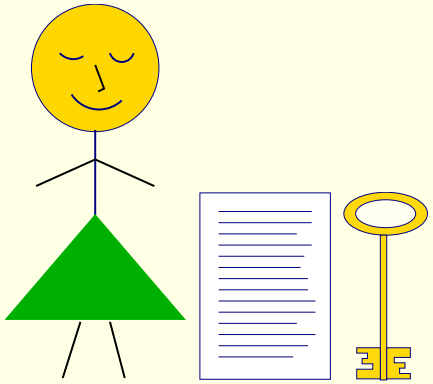
- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

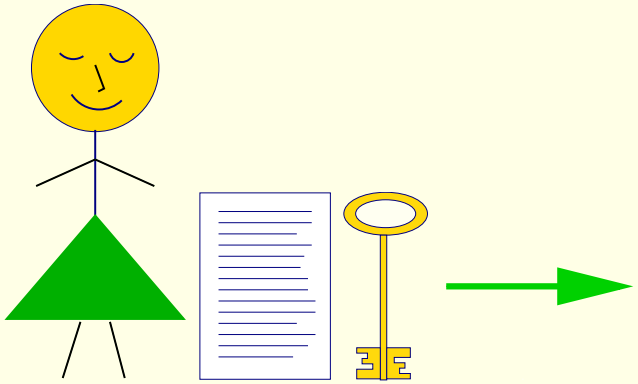
3 Współczesne kryptosystemy

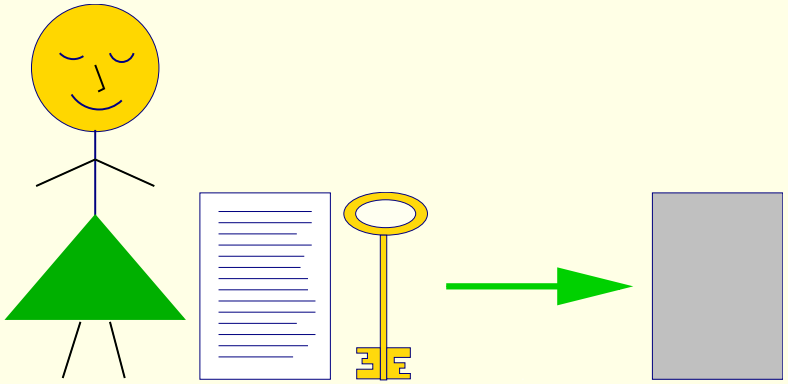
3.1 Systemy z kluczem tajnym

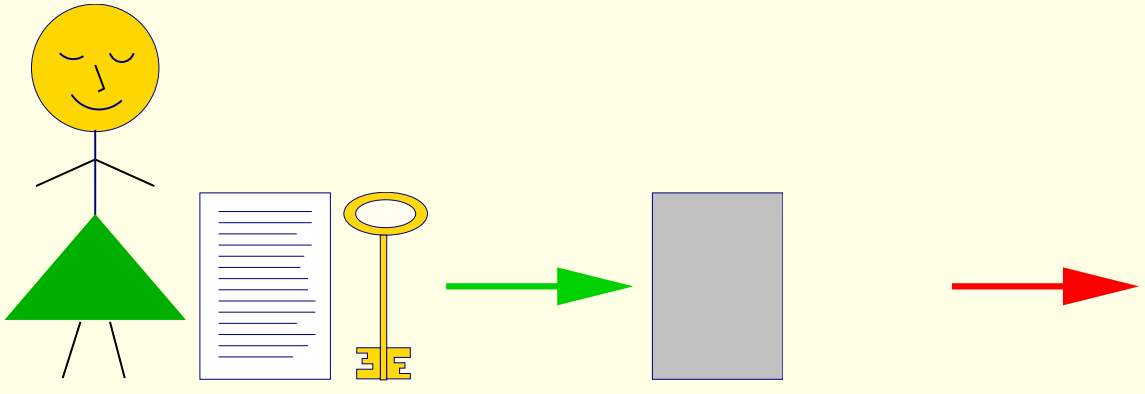


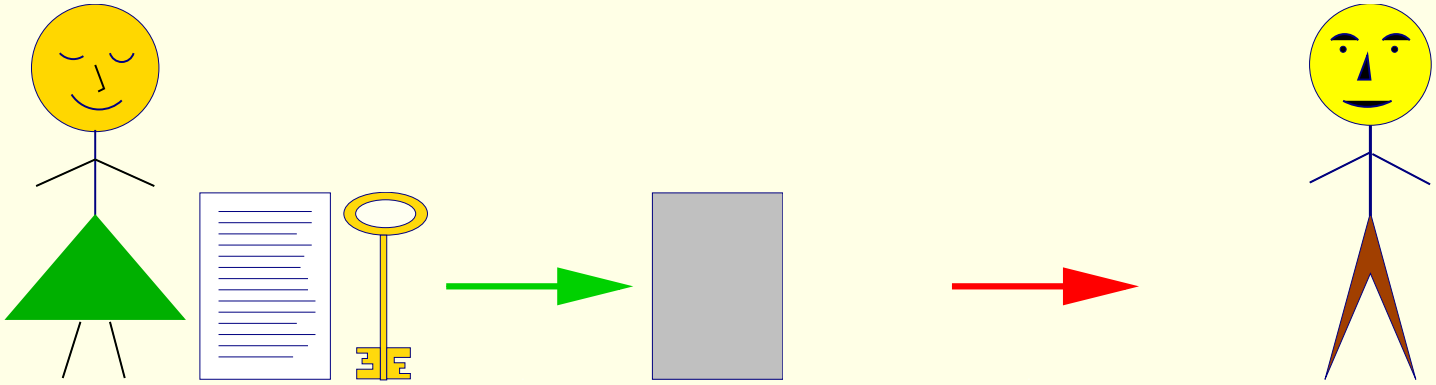


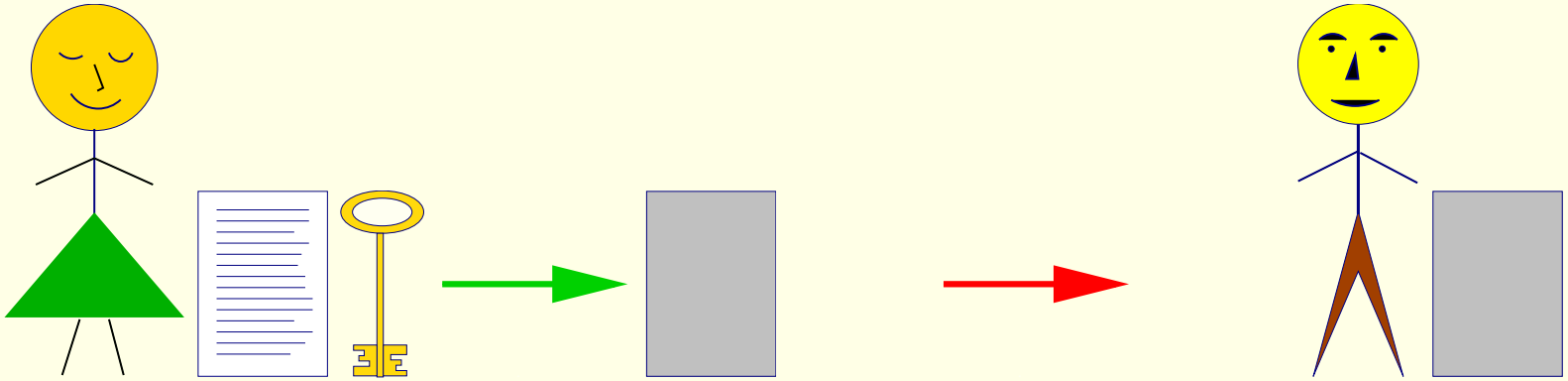


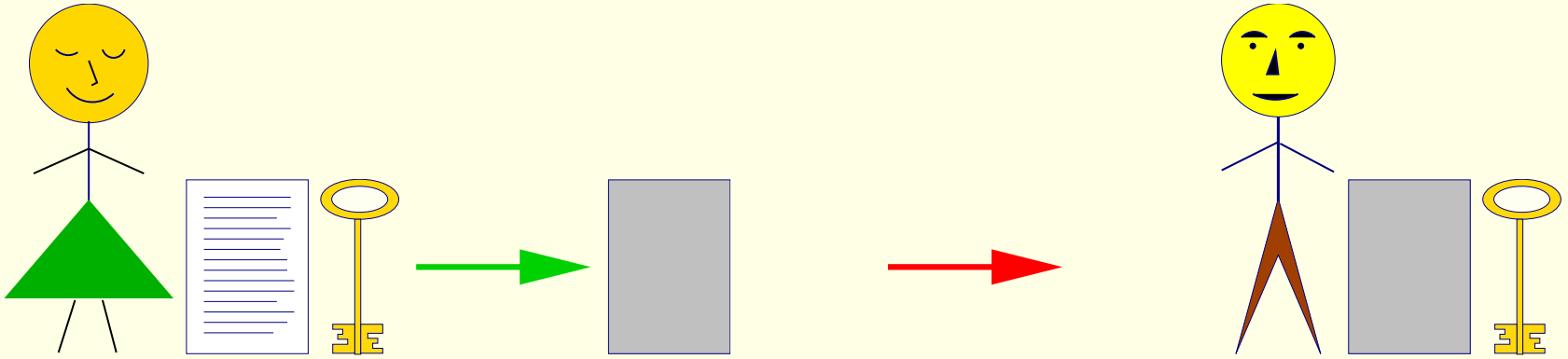


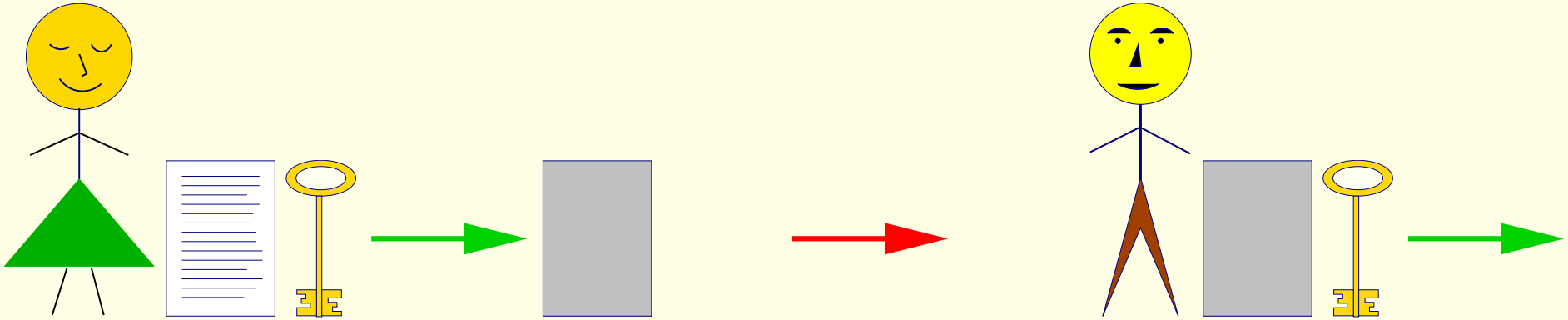


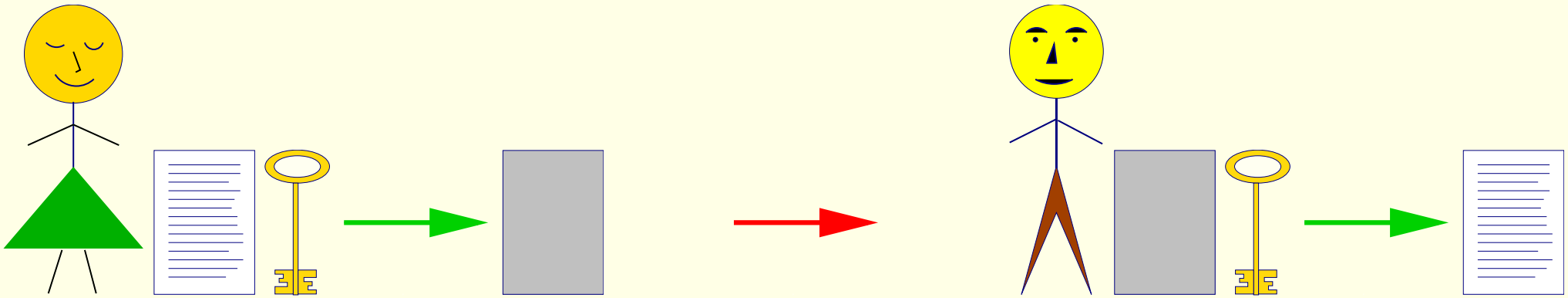


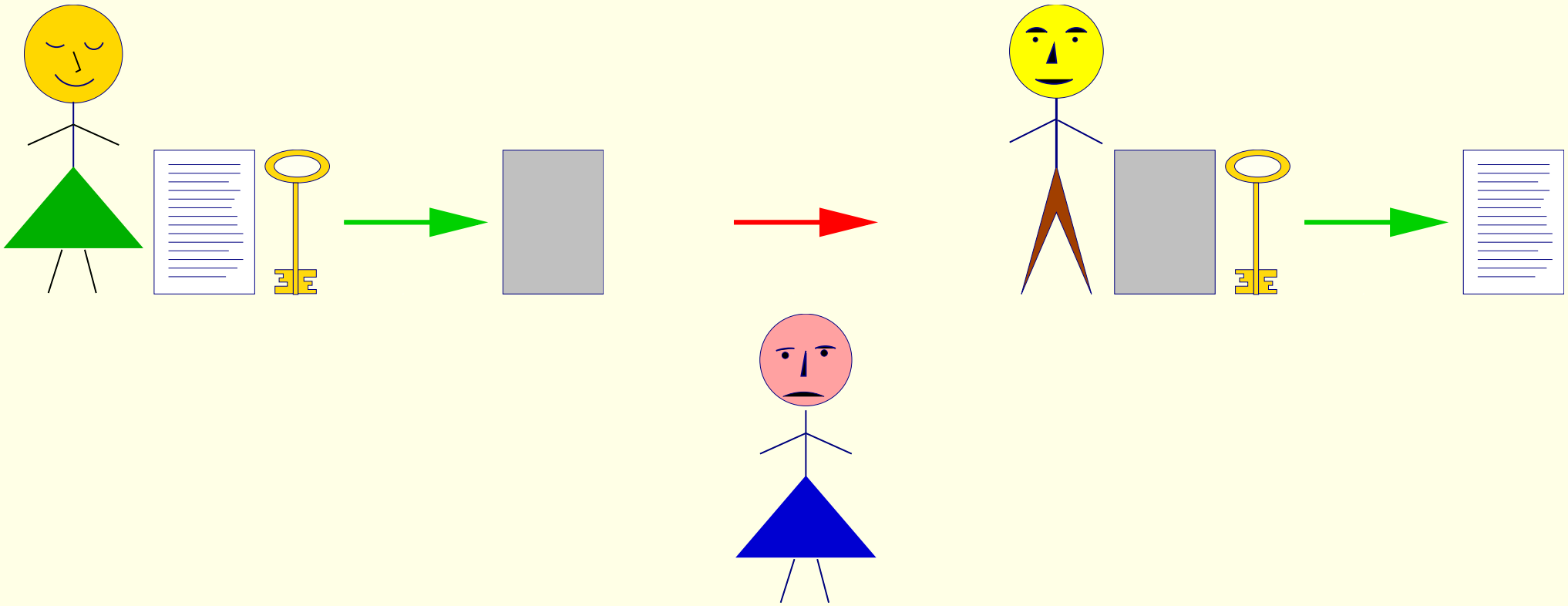


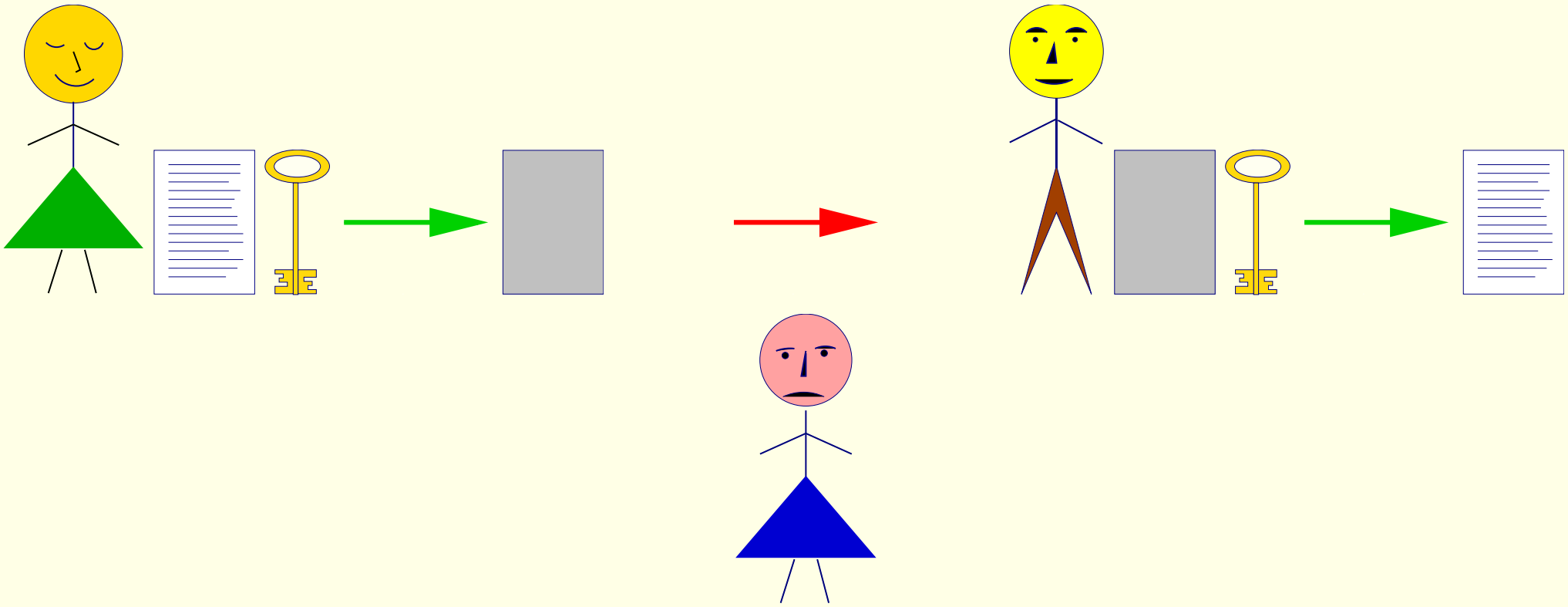


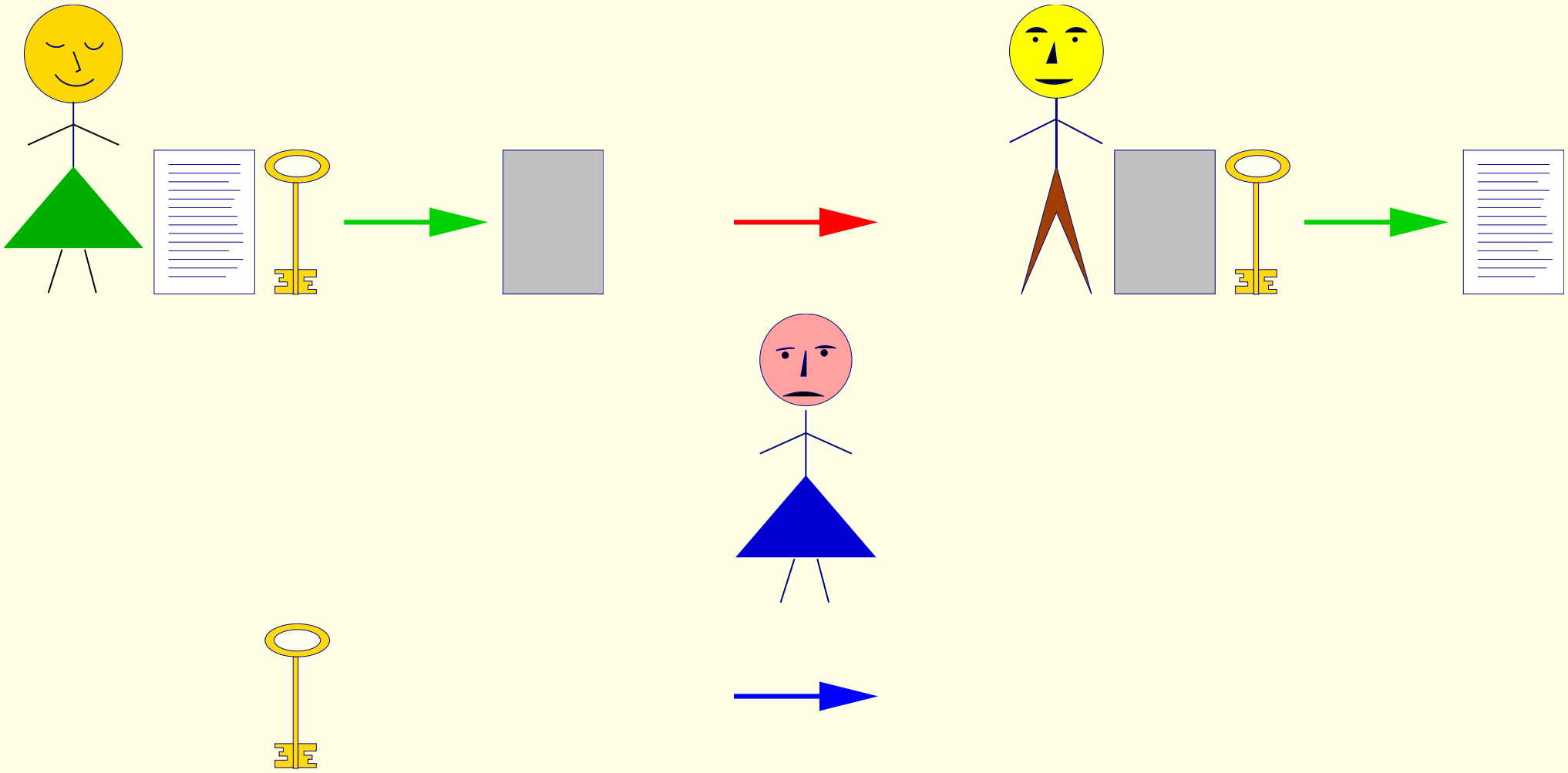


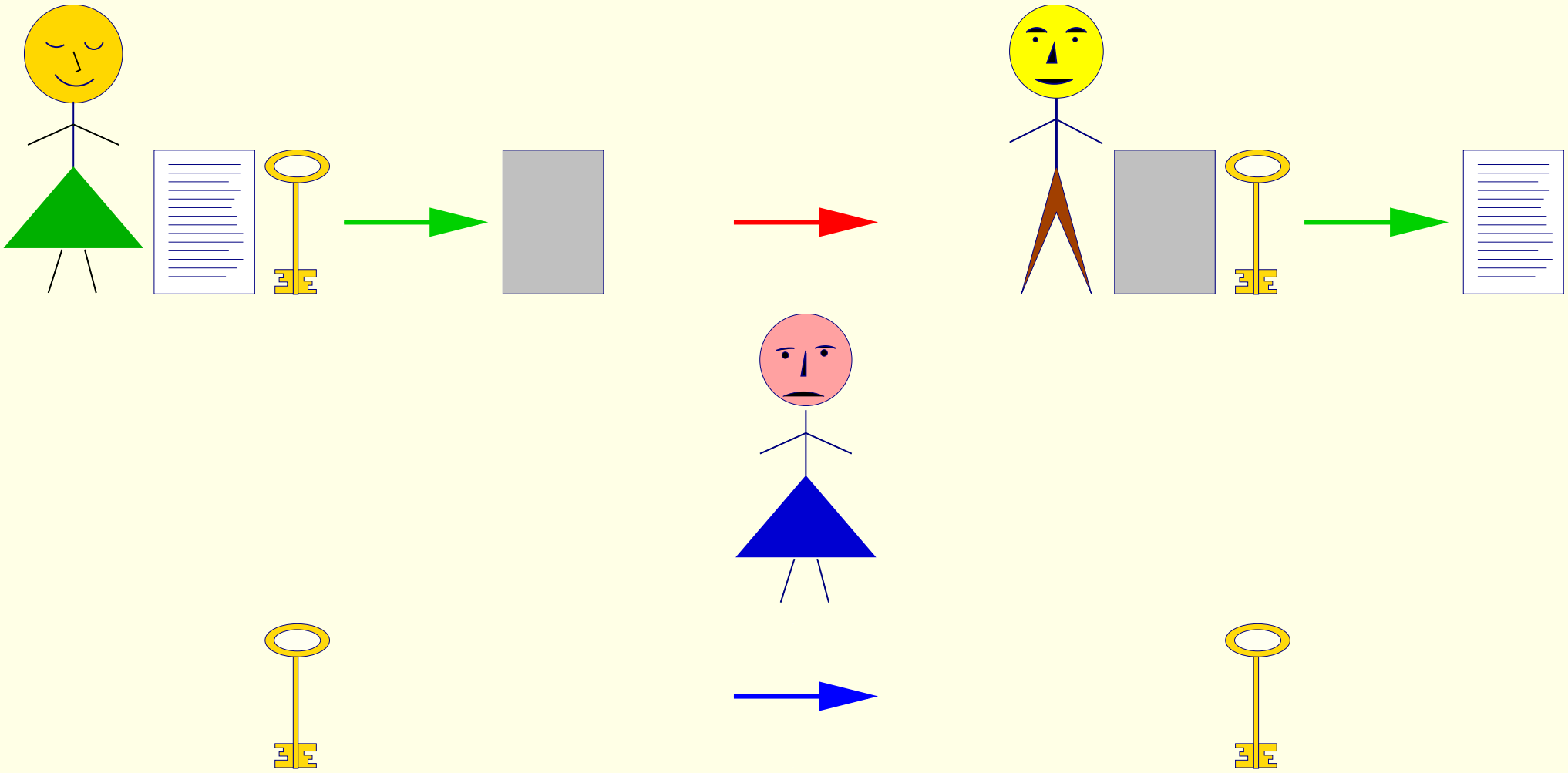


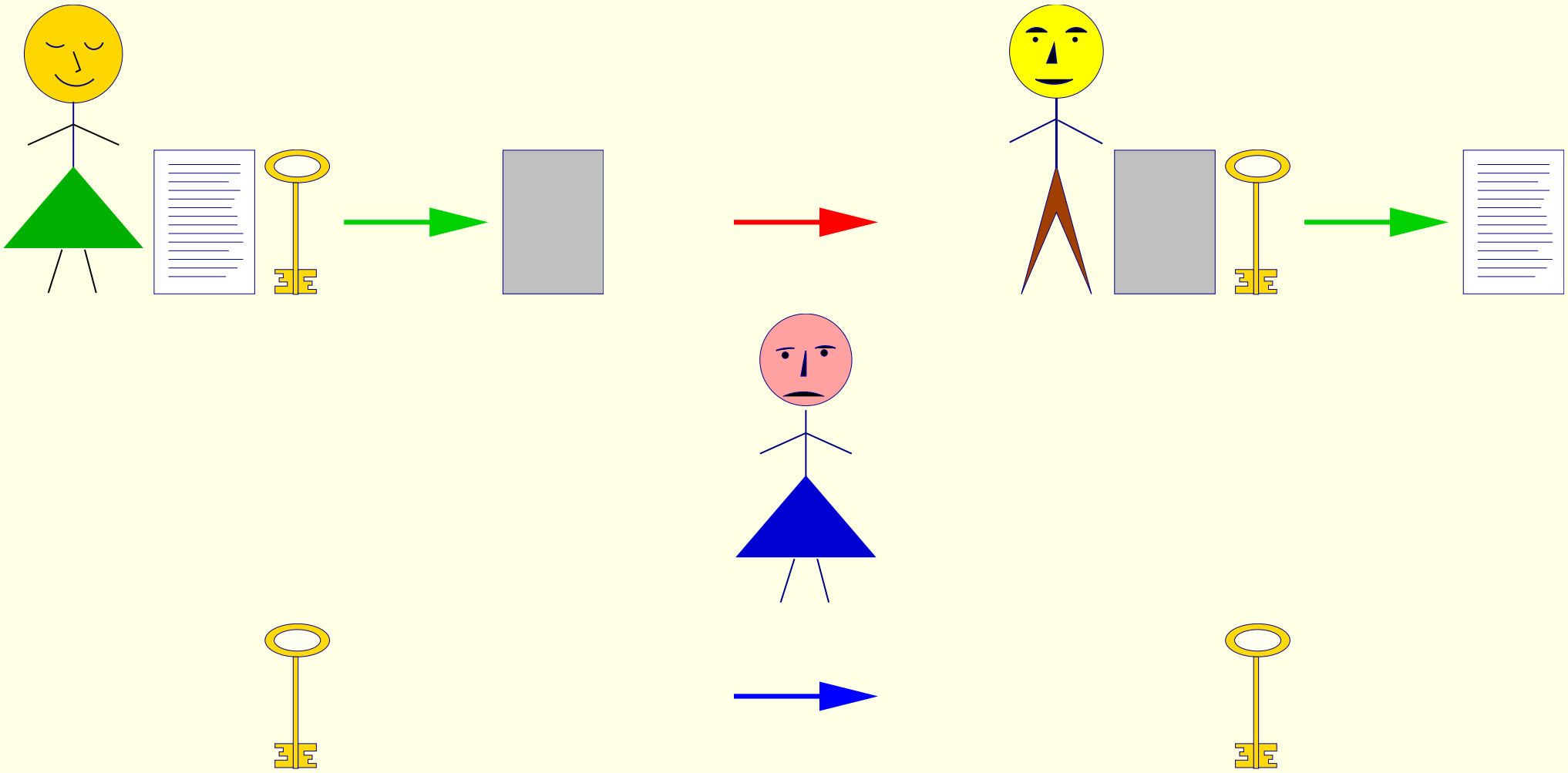








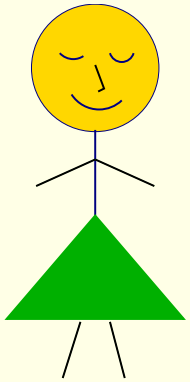


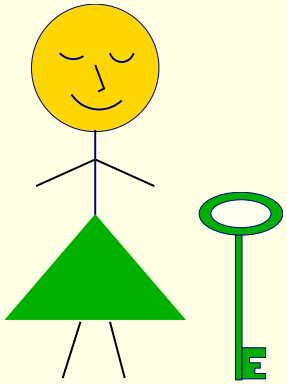


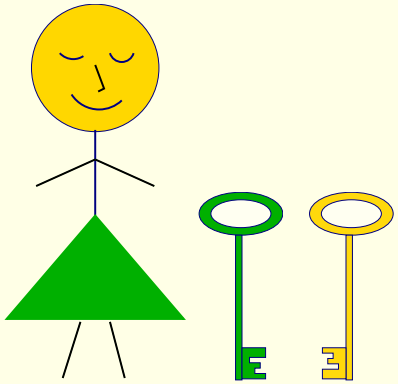
Pułapka

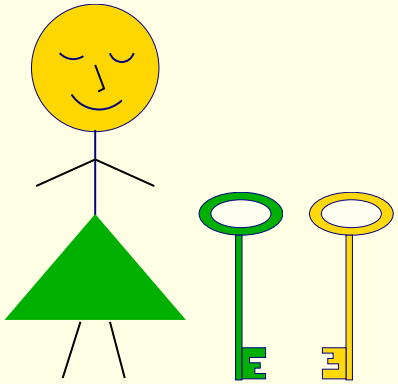
Aby zbudować bezpieczny kanał łączności trzeba mieć bezpieczny kanał łączności ...

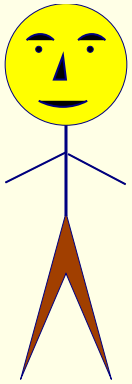
3.2 Systemy z kluczem publicznym

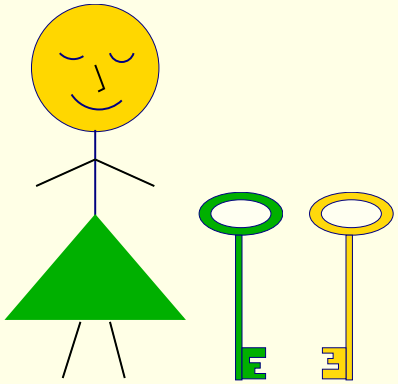


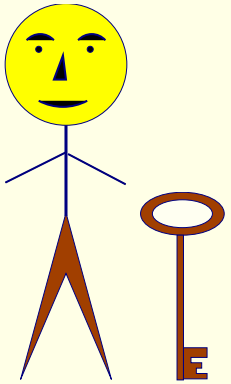


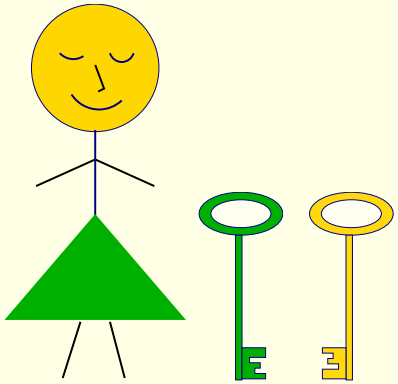


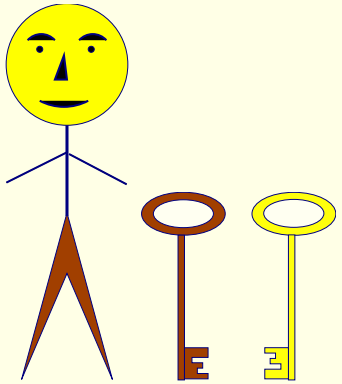


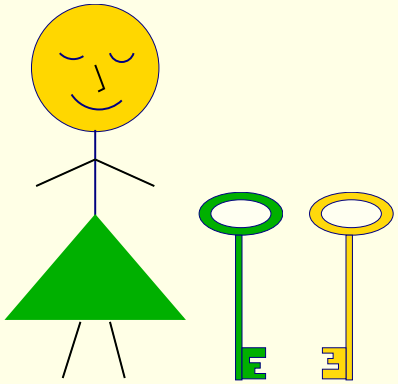




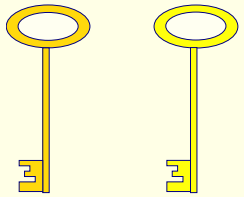




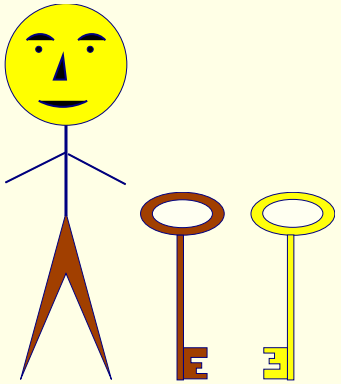


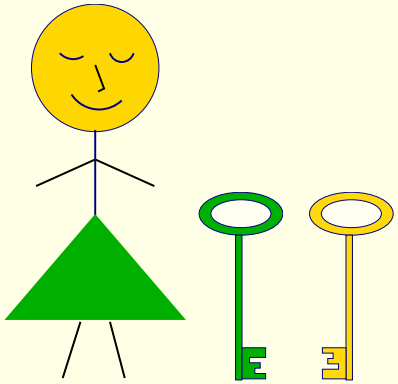


Klucze

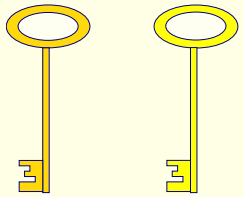


publiczne

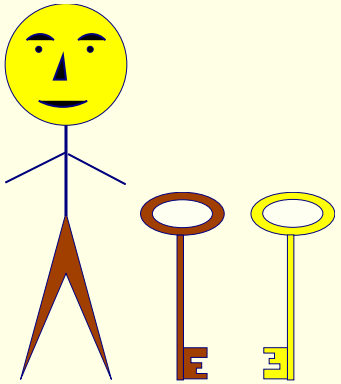


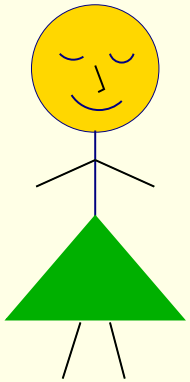


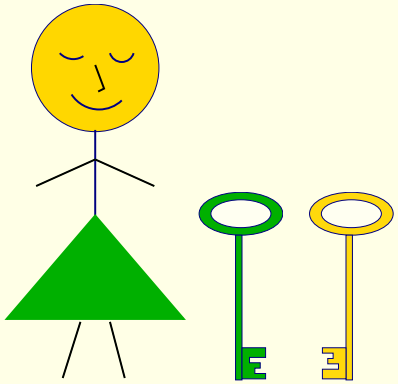
Klucze



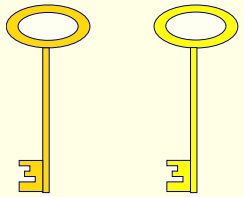
publiczne



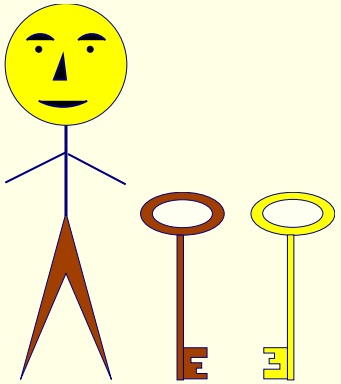


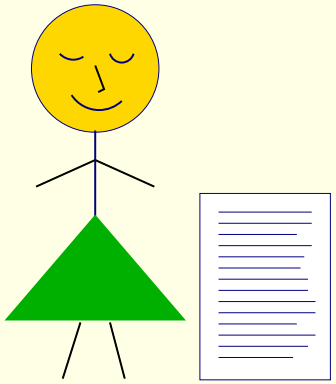


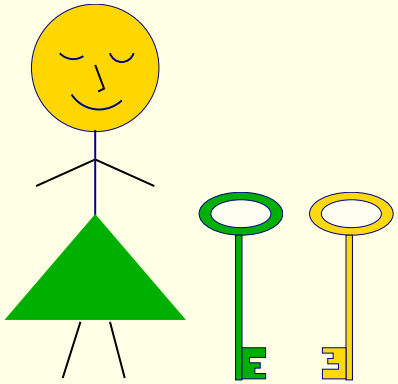
Klucze



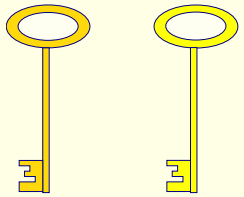
publiczne



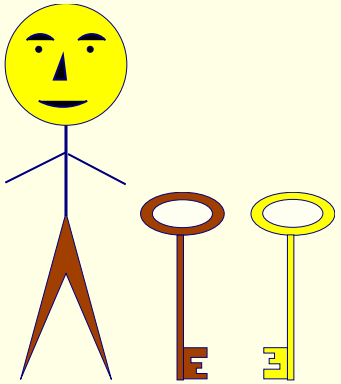


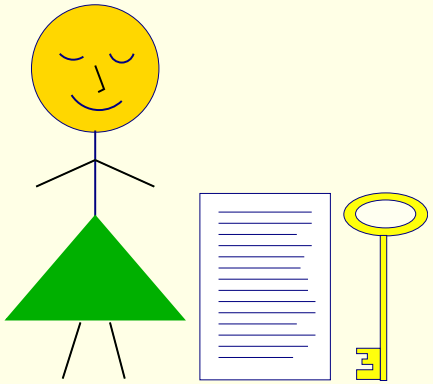


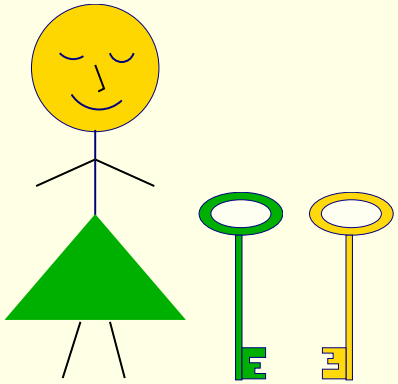
Klucze



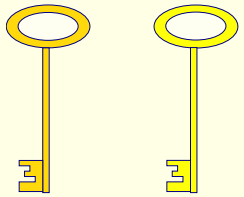
publiczne



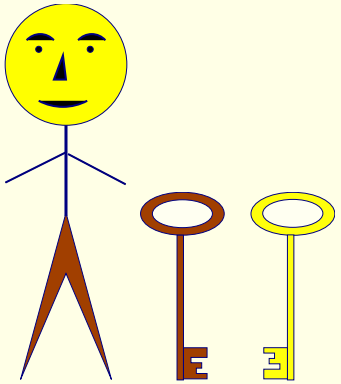


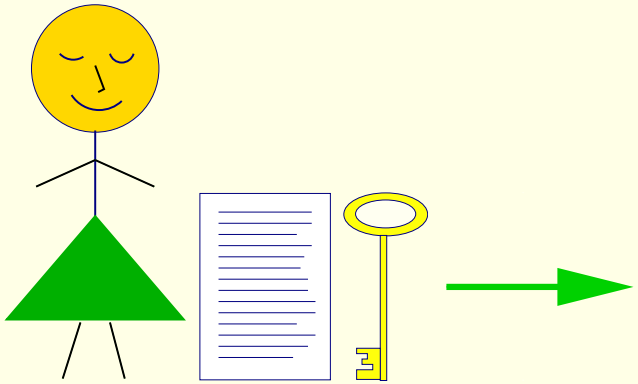


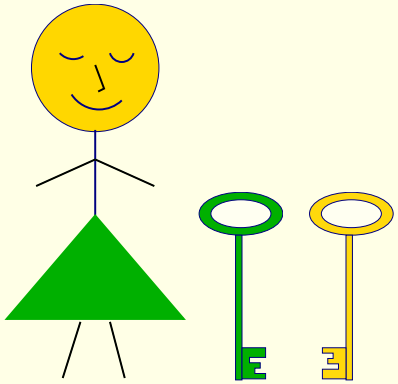
Klucze



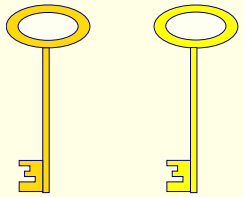
publiczne



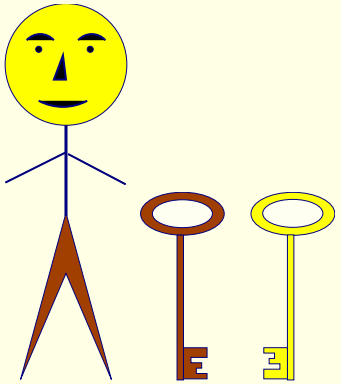


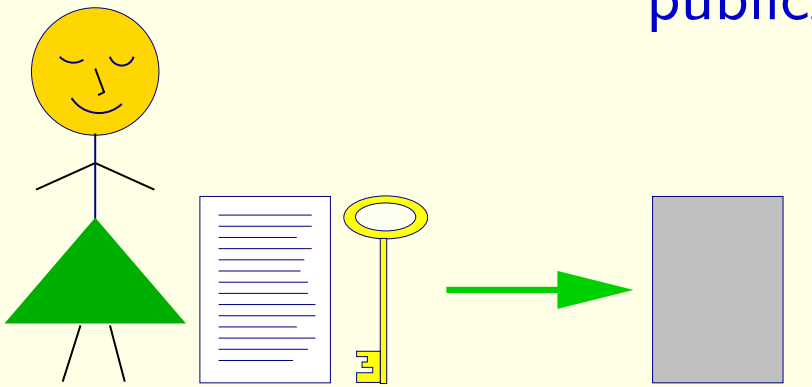


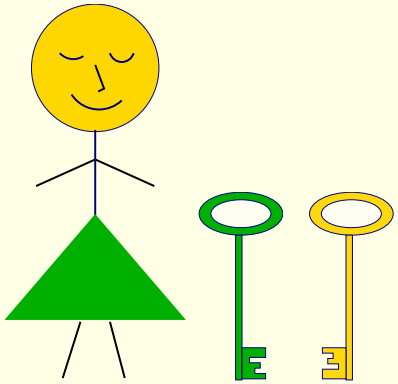
Klucze

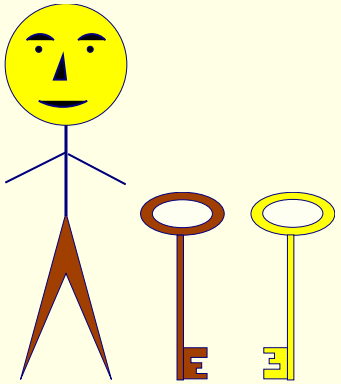


publiczne

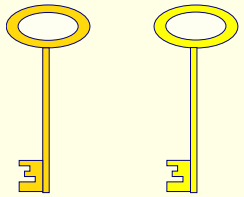




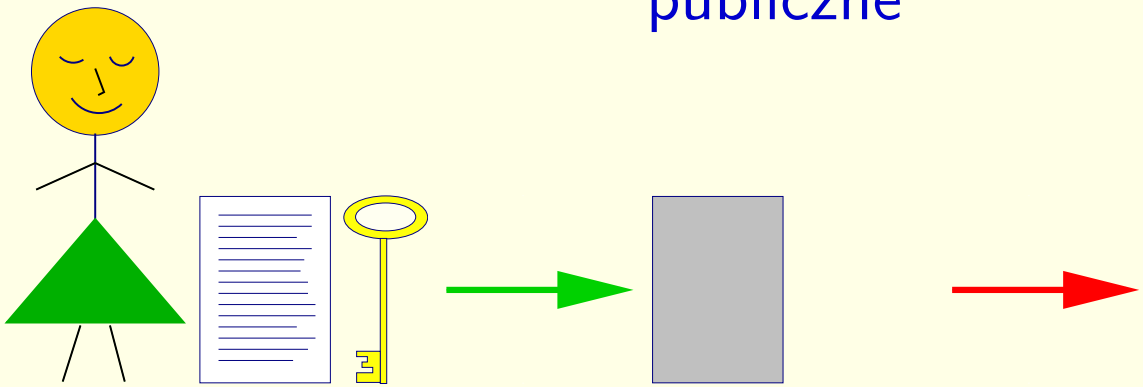


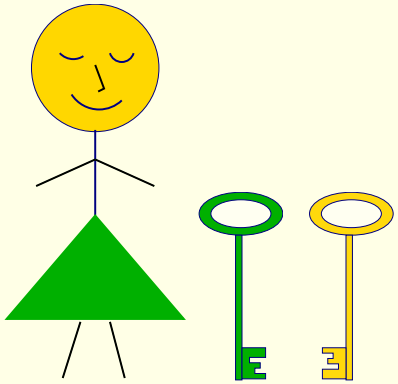


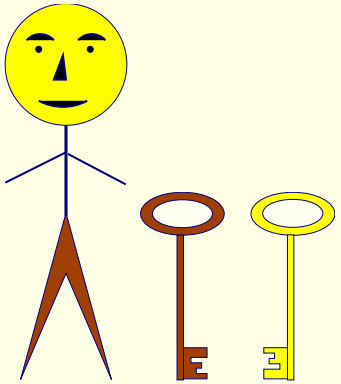
Klucze



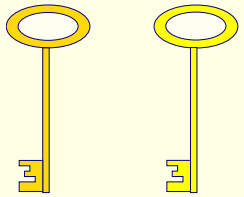
publiczne



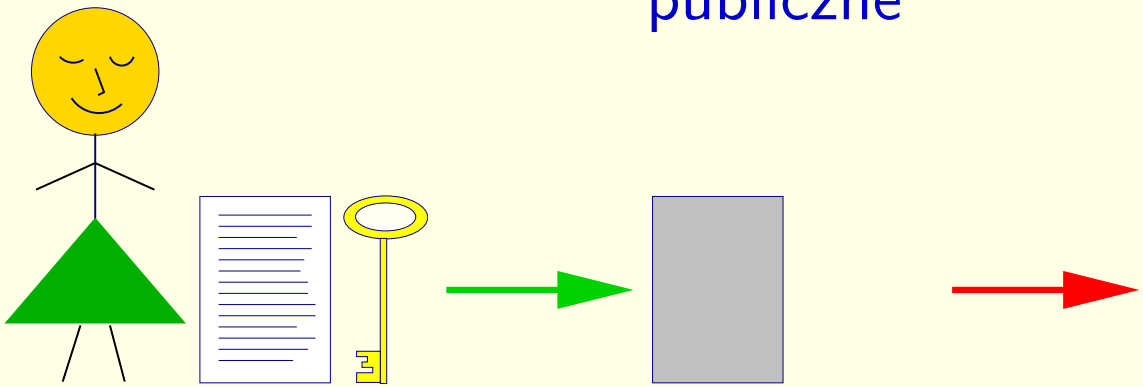


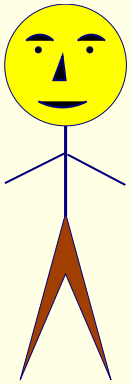


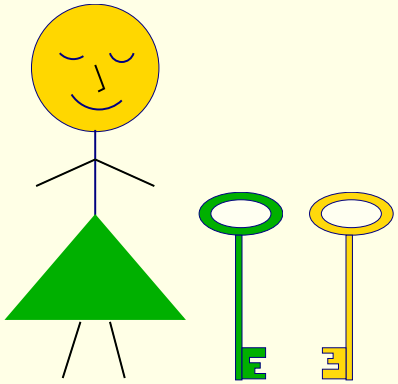
Klucze

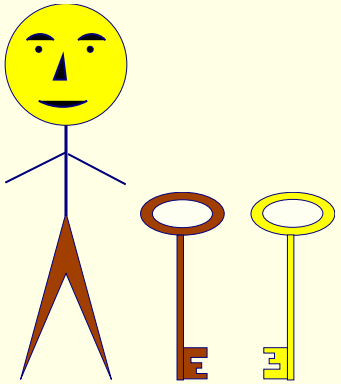


publiczne

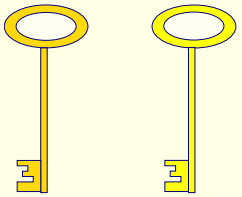




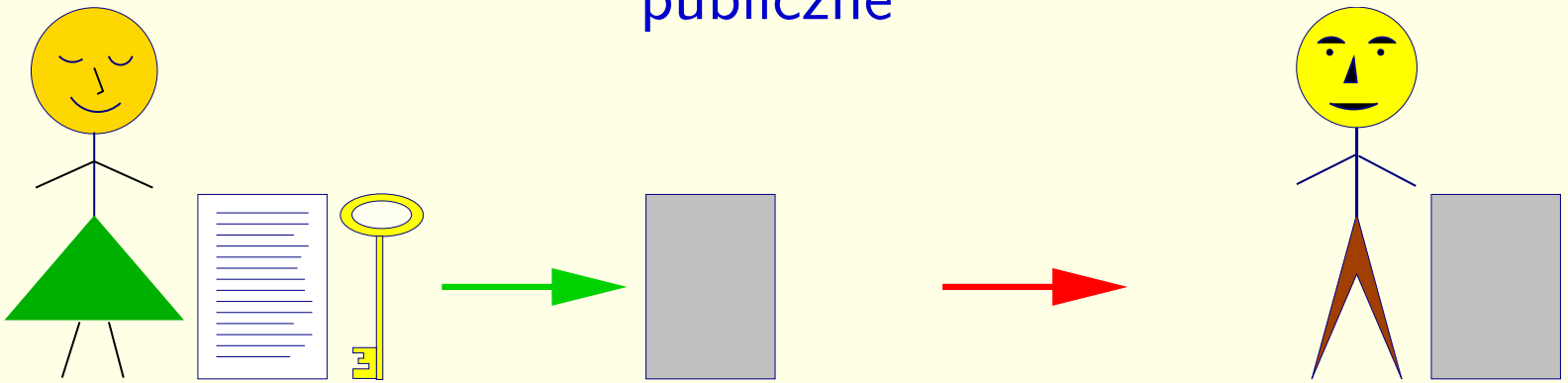


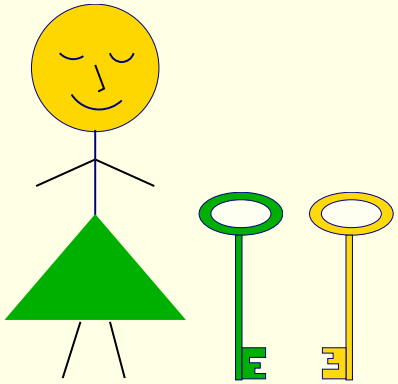


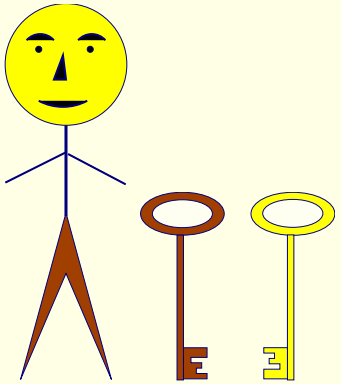
Klucze



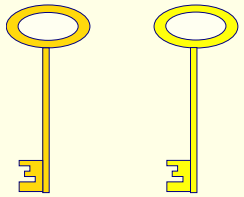
publiczne



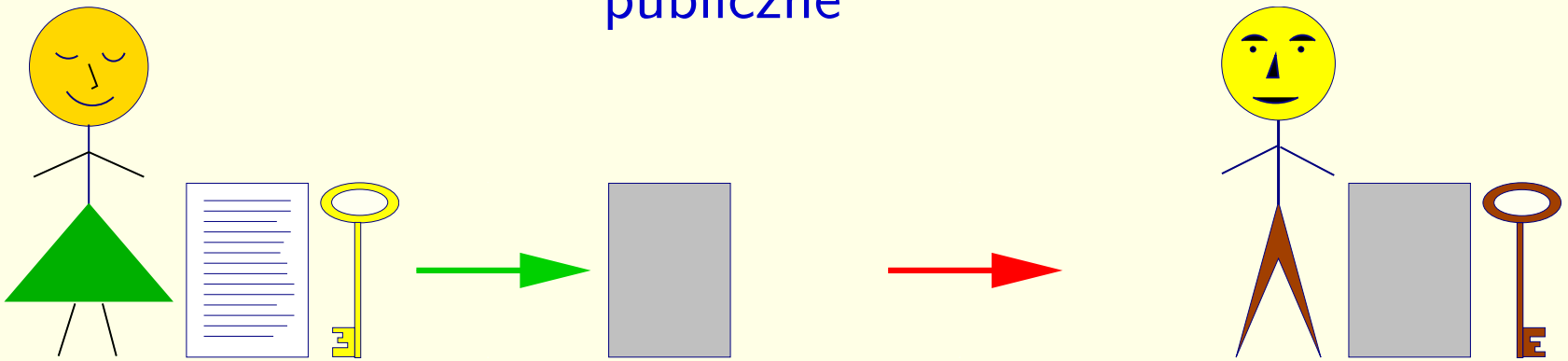


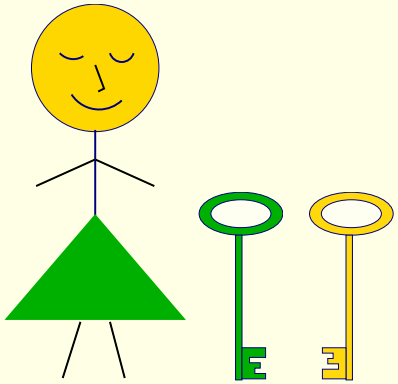


Klucze

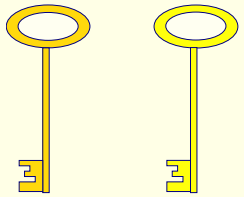


publiczne

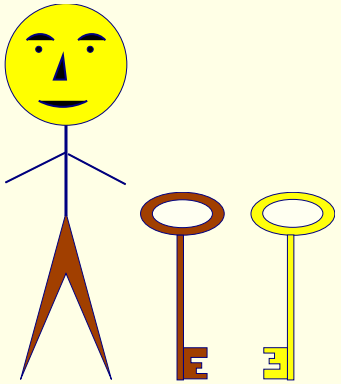


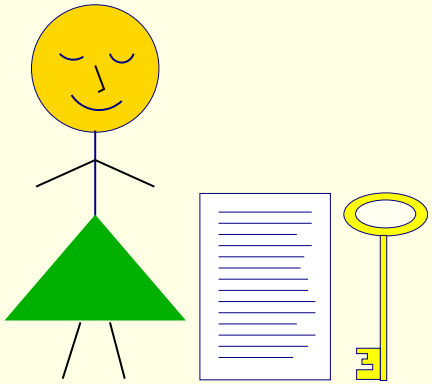


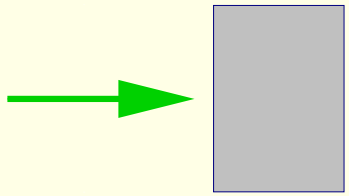
Klucze

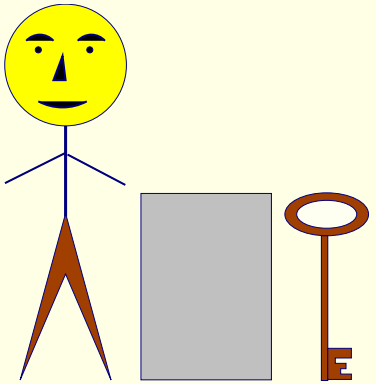


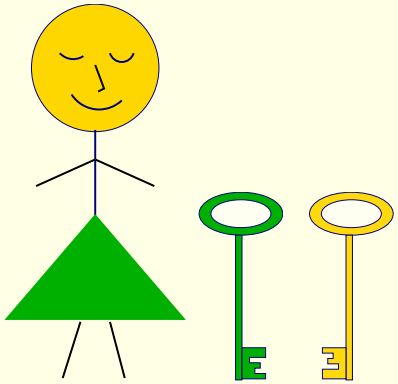
publiczne

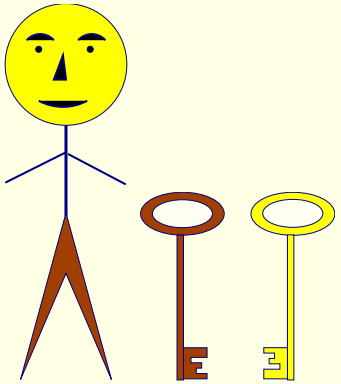




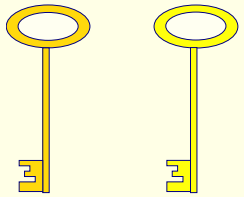




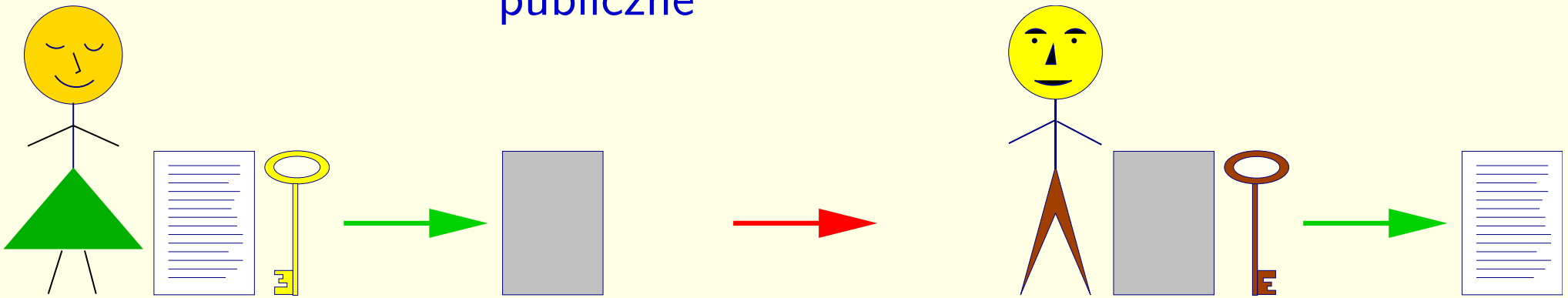


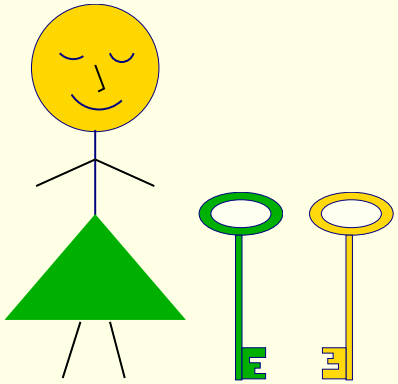


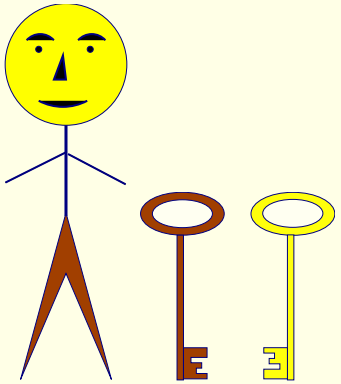
Klucze



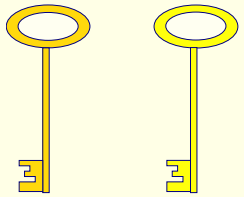
publiczne



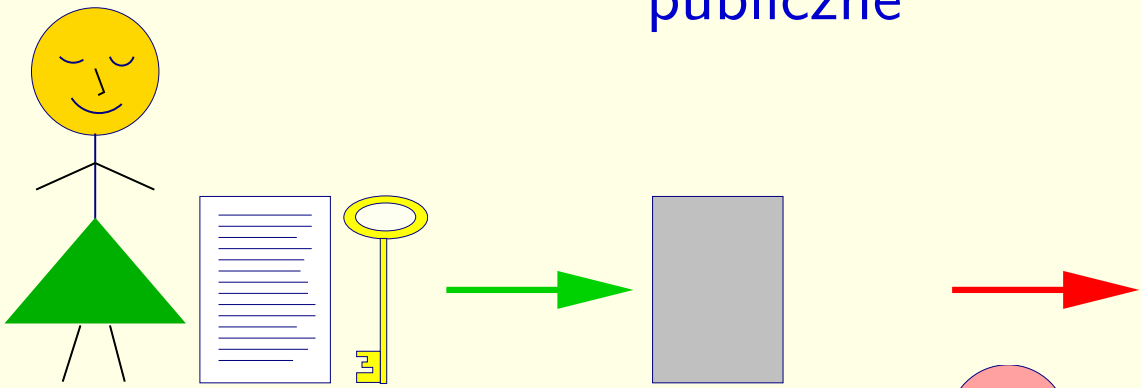


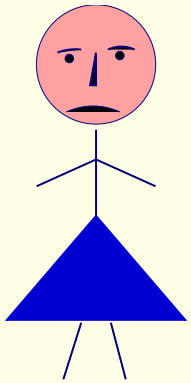


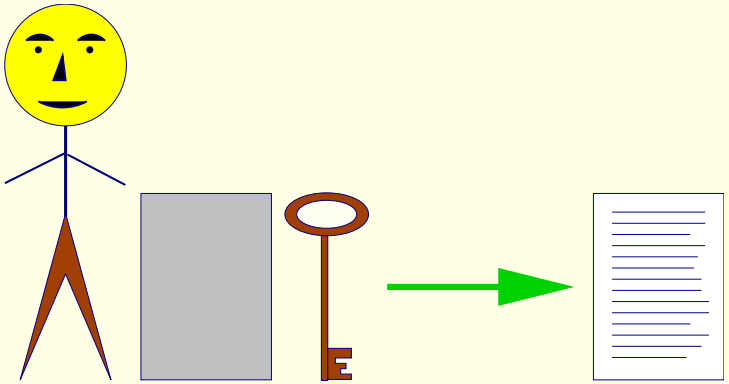
Klucze

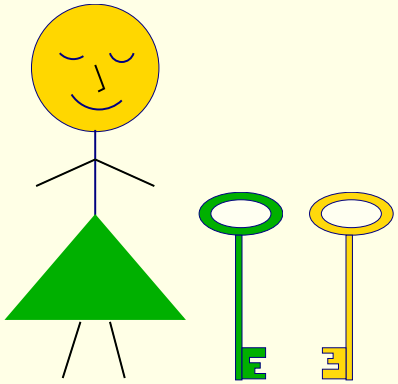


publiczne

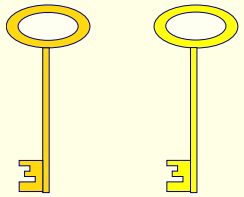




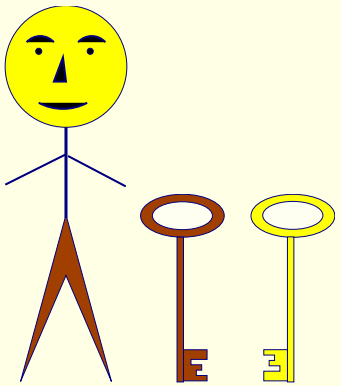


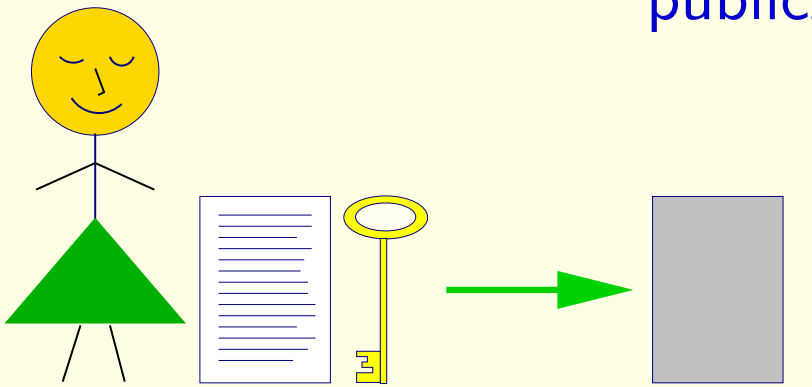


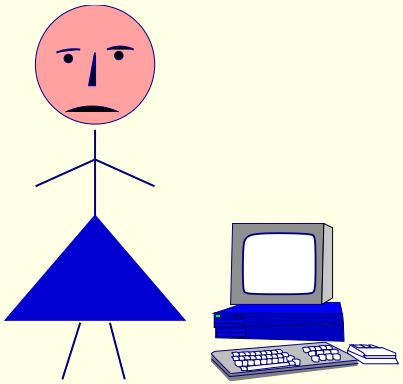
Klucze

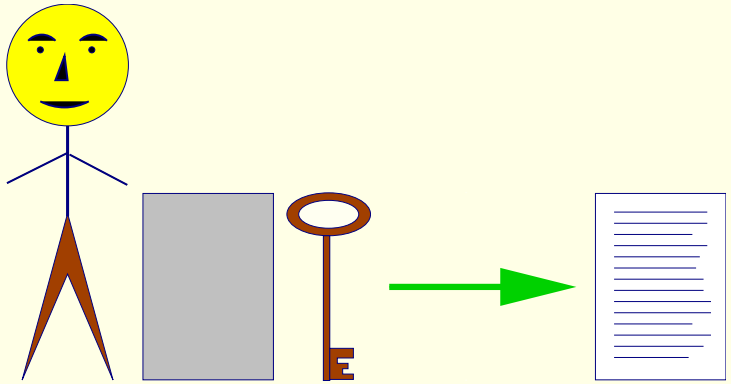


publiczne









Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

Jak to działa?

- Alicja i Bolek generują pary kluczy: jeden publiczny i jeden prywatny. Klucz publiczny udostępniają publicznie a prywatny skrzętnie chronią.
- Aby wysłać wiadomość do Bolka, Alicja bierze publiczny klucz Bolka, szyfuje nim wiadomość i kryptogram wysyła do Bolka.
- Bolek deszyfruje otrzymany kryptogram swoim kluczem prywatnym
- Nie ma potrzeby przesyłania tajnego klucza!
- Znakomicie! Nic lepszego nie potrzebujemy!

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja)

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja)

  Weźmy np liczbę

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja)

  Weźmy np liczbę

$$29083 \quad = \quad \square \cdot \square$$

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja)

  Weźmy np liczbę

$$29083 = \square \cdot \square$$

$$29083 =$$

A jednak!?

- Bezpieczeństwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartości samej funkcji jest łatwe zaś znalezienie argumentu funkcji kiedy znamy jej wartość jest obliczeniowo trudne (jak trudne to zależy od aktualnego stanu wiedzy i rozwoju techniki)
- Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera się na trudności z rozkładem liczby na czynniki (faktoryzacja)

  Weźmy np liczbę

$$29083 = \square \cdot \square$$

$$29083 = 127 \cdot 229$$

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.

  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.

  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.

  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.

  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!

- Czy jest jakieś wyjście?

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.

  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!
- Czy jest jakieś wyjście?
- Tak! Kryptografia kwantowa!

- Systemy takie nie gwarantują pełnego bezpieczeństwa. Nie można wykluczyć, że ktoś znajdzie efektywny algorytm faktoryzacji liczb.

  W istocie taki algorytm już istnieje.

  Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

  Trwają intensywne prace nad konstrukcją takiego komputera!

- Ewa wyposażona w komputer kwantowy z łatwością złamie szyfr RSA!
- Czy jest jakieś wyjście?
- Tak! Kryptografia kwantowa!

Ale o tym później!

4 Kryptografia bardziej formalnie

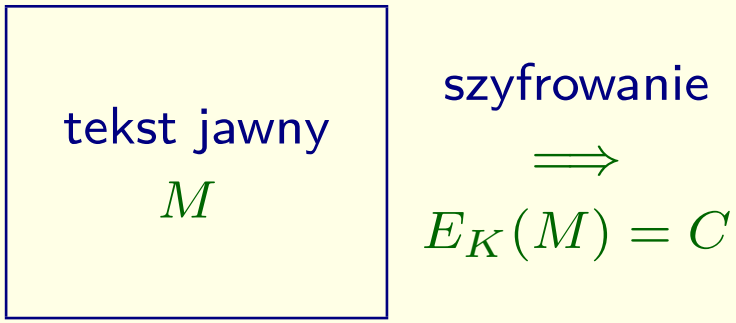
4.1 Szyfrowanie i deszyfrowanie

4 Kryptografia bardziej formalnie

4.1 Szyfrowanie i deszyfrowanie

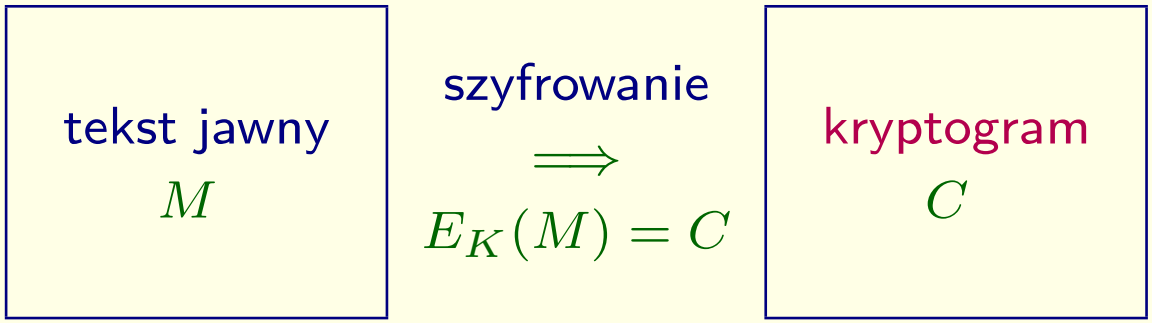
4 Kryptografia bardziej formalnie

4.1 Szyfrowanie i deszyfrowanie



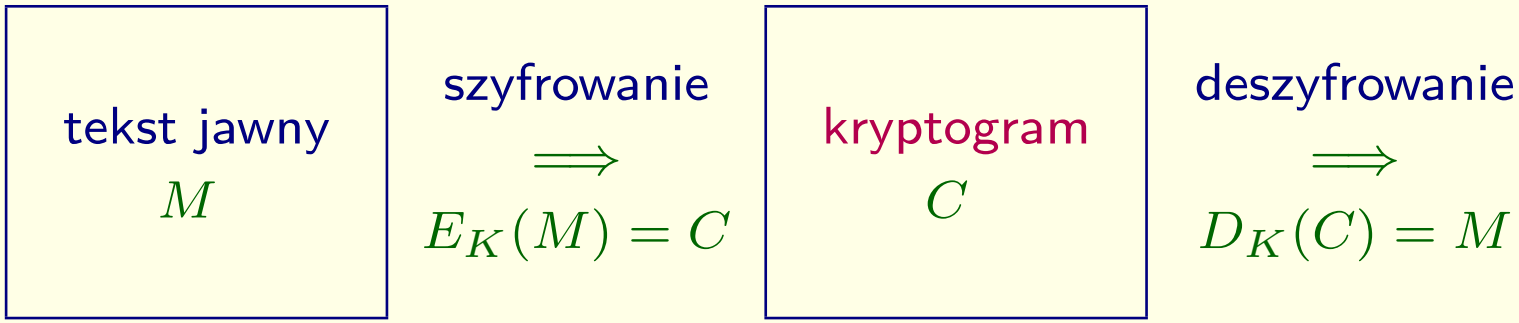
4 Kryptografia bardziej formalnie

4.1 Szyfrowanie i deszyfrowanie



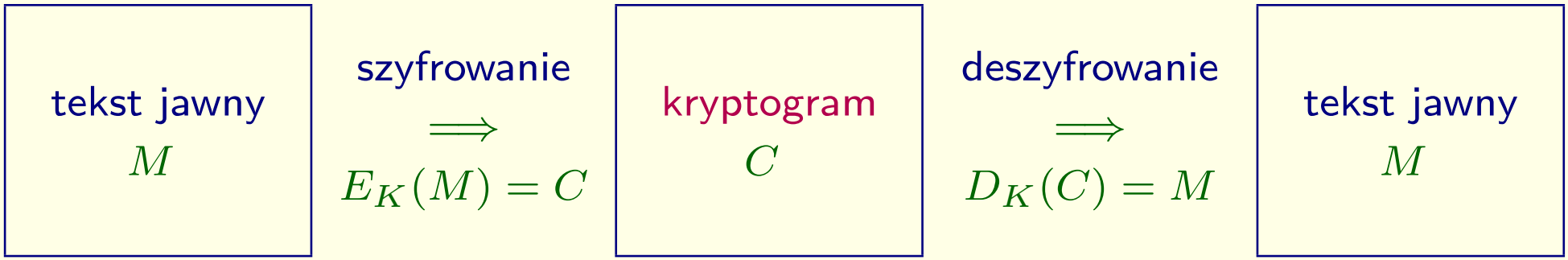
4 Kryptografia bardziej formalnie

4.1 Szyfrowanie i deszyfrowanie



4 Kryptografia bardziej formalnie

4.1 Szyfrowanie i deszyfrowanie



4.2 Algorytmy

- symetryczne — klucz do szyfrowania i deszyfrowania jest ten sam

  klucz tajny — DES, IDEA, AES

- asymetryczne — klucze do szyfrowania i deszyfrowania są różne

  klucz jawny albo publiczny — RSA, ElGamal

4.2 Algorytmy

- symetryczne — klucz do szyfrowania i deszyfrowania jest ten sam

  klucz tajny — DES, IDEA, AES

- asymetryczne — klucze do szyfrowania i deszyfrowania są różne

  klucz jawny albo publiczny — RSA, ElGamal

4.2 Algorytmy

- symetryczne — klucz do szyfrowania i deszyfrowania jest ten sam

  klucz tajny — DES, IDEA, AES

- asymetryczne — klucze do szyfrowania i deszyfrowania są różne

  klucz jawny albo publiczny — RSA, ElGamal

4.3 Przykład kryptogramu

- tekst jawny

  Wykład z podstaw klasycznej kryptografii z elementami kryptografii kwantowej

4.3 Przykład kryptogramu

- tekst jawny

> Wykład z podstaw klasycznej kryptografii z elementami kryptografii kwantowej

- kryptogram (GnuPG)

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: Dalsze informacje znajdują się na http://www.gnupg.org/

hQEOA+npwcy1l0+VEAP+IrpTozmtpWBINXV5koW5sBC86EAelZTrEXrzUHohenPo
ohzkgIoBH17Rvu46hZUsHjeHyH74RI1Lv0klHbtBOLiCLvZfdtBWFFtzr4j4kDt7
n7kGMrJCxwOKuZIVCdMrRS9jvcBgFydYIeq/jkA3VvPGU4nT3AEyqiZ+xkrPRvsE
AJ59+4YDc1sbccJdu6nyRMJ2rcYH+SoS+BDgUmkopkG2KCjnQHArUWGq9N1v3ULH
dRfKwl4kgOK2EQGTFaQxjGXqyK41MS5noOZhZ8nHgJ4N9vE/TH/CaTiWgLQyXoKt
4J4xOJ5wx6rjNIK5MRl37XxWr3D8xDwWBGtKFGLllcV/0ogBymNlqBWZB6qi/xZo
cLdPWR94WmIvpkxWsR5HZhU06K6D7l/KgSarosSDwpOtT6c/21epCZvuvrfnq8pm
lpTXqVuHVsZNGCp599pJCkgLTxdQDyV0xjD8feVEtX2pfHxdWMORMdEG2QGfWSCa
z0hvf2t7B+7lFQsK+TPi3+YQMaoXK+XmAyPz
=vRaX
-----END PGP MESSAGE-----
```

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.4 Podstawowe zastosowania

- ochrona danych
  - dane na dyskach
  - przesyłanie danych poprzez linie narażone na podsłuch
- uwierzytelnianie dokumentów i osób
- ochrona prywatności korespondencji elektronicznej
- elektroniczny notariusz
- podpis cyfrowy
- pieniądze cyfrowe
- wybory elektroniczne

4.5 Jak to działa: algorytm symetryczny

- Alicja i Bolek uzgadniają algorytm i klucz jakich będą używać
- Alicja szyfruje tekst używając uzgodnionego algorytmu i klucza otrzymując kryptogram
- Alicja przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając tego samego algorytmu i klucza otrzymując tekst jawny

4.5 Jak to działa: algorytm symetryczny

- Alicja i Bolek uzgadniają algorytm i klucz jakich będą używać
- Alicja szyfruje tekst używając uzgodnionego algorytmu i klucza otrzymując kryptogram
- Alicja przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając tego samego algorytmu i klucza otrzymując tekst jawny

4.5 Jak to działa: algorytm symetryczny

- Alicja i Bolek uzgadniają algorytm i klucz jakich będą używać
- Alicja szyfruje tekst używając uzgodnionego algorytmu i klucza otrzymując kryptogram
- Alicja przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając tego samego algorytmu i klucza otrzymując tekst jawny

4.5 Jak to działa: algorytm symetryczny

- Alicja i Bolek uzgadniają algorytm i klucz jakich będą używać
- Alicja szyfruje tekst używając uzgodnionego algorytmu i klucza otrzymując kryptogram
- Alicja przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając tego samego algorytmu i klucza otrzymując tekst jawny

4.5 Jak to działa: algorytm symetryczny

- Alicja i Bolek uzgadniają algorytm i klucz jakich będą używać
- Alicja szyfruje tekst używając uzgodnionego algorytmu i klucza otrzymując kryptogram
- Alicja przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając tego samego algorytmu i klucza otrzymując tekst jawny

- Problemy:
  - klucz musi być przekazywany w sposób tajny
  - jeśli Ewa wejdzie w posiadanie klucza to może deszyfrować wszystko, a nawet podszyć się pod Alicję
  - jeśli każda para korespondentów w sieci dysponuje własnym kluczem to liczba kluczy szybko rośnie dla kogoś kto utrzymuje kontakt z wieloma osobami

- Problemy:
  - klucz musi być przekazywany w sposób tajny
  - jeśli Ewa wejdzie w posiadanie klucza to może deszyfrować wszystko, a nawet podszyć się pod Alicję
  - jeśli każda para korespondentów w sieci dysponuje własnym kluczem to liczba kluczy szybko rośnie dla kogoś kto utrzymuje kontakt z wieloma osobami

- Problemy:
  - klucz musi być przekazywany w sposób tajny
  - jeśli Ewa wejdzie w posiadanie klucza to może deszyfrować wszystko, a nawet podszyć się pod Alicję
  - jeśli każda para korespondentów w sieci dysponuje własnym kluczem to liczba kluczy szybko rośnie dla kogoś kto utrzymuje kontakt z wieloma osobami

- Problemy:
  - klucz musi być przekazywany w sposób tajny
  - jeśli Ewa wejdzie w posiadanie klucza to może deszyfrować wszystko, a nawet podszyć się pod Alicję
  - jeśli każda para korespondentów w sieci dysponuje własnym kluczem to liczba kluczy szybko rośnie dla kogoś kto utrzymuje kontakt z wieloma osobami

4.6 Jak to działa: algorytm asymetryczny

- Alicja i Bolek uzgadniają kryptosystem z kluczem publicznym, którego będą używać
- Bolek przesyła Alicji swój klucz publiczny
- Alicja szyfruje wiadomość kluczem publicznym Bolka i przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając swojego klucza prywatnego

4.6 Jak to działa: algorytm asymetryczny

- Alicja i Bolek uzgadniają kryptosystem z kluczem publicznym, którego będą używać
- Bolek przesyła Alicji swój klucz publiczny
- Alicja szyfruje wiadomość kluczem publicznym Bolka i przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając swojego klucza prywatnego

4.6 Jak to działa: algorytm asymetryczny

- Alicja i Bolek uzgadniają kryptosystem z kluczem publicznym, którego będą używać
- Bolek przesyła Alicji swój klucz publiczny
- Alicja szyfruje wiadomość kluczem publicznym Bolka i przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając swojego klucza prywatnego

4.6 Jak to działa: algorytm asymetryczny

- Alicja i Bolek uzgadniają kryptosystem z kluczem publicznym, którego będą używać
- Bolek przesyła Alicji swój klucz publiczny
- Alicja szyfruje wiadomość kluczem publicznym Bolka i przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając swojego klucza prywatnego

4.6 Jak to działa: algorytm asymetryczny

- Alicja i Bolek uzgadniają kryptosystem z kluczem publicznym, którego będą używać
- Bolek przesyła Alicji swój klucz publiczny
- Alicja szyfruje wiadomość kluczem publicznym Bolka i przesyła kryptogram do Bolka
- Bolek deszyfruje kryptogram używając swojego klucza prywatnego

lub

użytkownicy sieci uzgadniają kryptosystem i przesyłają swoje klucze publiczne do bazy na znanym serwerze i wtedy protokół wygląda jeszcze prościej

- Alicja i Bolek pobierają klucze publiczne z serwera
- Alicja szyfruje wiadomość kluczem publicznym Bolka i wysyła kryptogram do Bolka
- Bolek deszyfruje wiadomość Alicji używając własnego klucza prywatnego

lub

użytkownicy sieci uzgadniają kryptosystem i przesyłają swoje klucze publiczne do bazy na znanym serwerze i wtedy protokół wygląda jeszcze prościej

- Alicja i Bolek pobierają klucze publiczne
  z serwera
- Alicja szyfruje wiadomość kluczem publicznym Bolka i wysyła kryptogram do Bolka
- Bolek deszyfruje wiadomość Alicji używając własnego klucza prywatnego

lub

użytkownicy sieci uzgadniają kryptosystem i przesyłają swoje klucze publiczne do bazy na znanym serwerze i wtedy protokół wygląda jeszcze prościej

- Alicja i Bolek pobierają klucze publiczne z serwera
- Alicja szyfruje wiadomość kluczem publicznym Bolka i wysyła kryptogram do Bolka
- Bolek deszyfruje wiadomość Alicji używając własnego klucza prywatnego

lub

użytkownicy sieci uzgadniają kryptosystem i przesyłają swoje klucze publiczne do bazy na znanym serwerze i wtedy protokół wygląda jeszcze prościej

- Alicja i Bolek pobierają klucze publiczne z serwera
- Alicja szyfruje wiadomość kluczem publicznym Bolka i wysyła kryptogram do Bolka
- Bolek deszyfruje wiadomość Alicji używając własnego klucza prywatnego

4.7 Kryptosystem hybrydowy

- Bolek wysyła do Alicji swój klucz publiczny
- Alicja generuje losowy klucz K dla obecnej sesji, szyfruje go kluczem publicznym Bolka i wysyła kryptogram klucza $E_B(K)$ do Bolka
- Bolek deszyfruje kryptogram klucza używając swojego klucza prywatnego, $D_B(E_B(K)) = K$, otrzymując klucz K dla obecnej sesji
- oboje używają klucza K i symetrycznego algorytmu do szyfrowania i deszyfrowania informacji przesyłanych w czasie tej sesji

4.7 Kryptosystem hybrydowy

- Bolek wysyła do Alicji swój klucz publiczny
- Alicja generuje losowy klucz K dla obecnej sesji, szyfruje go kluczem publicznym Bolka i wysyła kryptogram klucza $E_B(K)$ do Bolka
- Bolek deszyfruje kryptogram klucza używając swojego klucza prywatnego, $D_B(E_B(K)) = K$, otrzymując klucz K dla obecnej sesji
- oboje używają klucza K i symetrycznego algorytmu do szyfrowania i deszyfrowania informacji przesyłanych w czasie tej sesji

4.7 Kryptosystem hybrydowy

- Bolek wysyła do Alicji swój klucz publiczny
- Alicja generuje losowy klucz K dla obecnej sesji, szyfruje go kluczem publicznym Bolka i wysyła kryptogram klucza $E_B(K)$ do Bolka
- Bolek deszyfruje kryptogram klucza używając swojego klucza prywatnego, $D_B(E_B(K)) = K$, otrzymując klucz K dla obecnej sesji
- oboje używają klucza K i symetrycznego algorytmu do szyfrowania i deszyfrowania informacji przesyłanych w czasie tej sesji

4.7 Kryptosystem hybrydowy

- Bolek wysyła do Alicji swój klucz publiczny
- Alicja generuje losowy klucz K dla obecnej sesji, szyfruje go kluczem publicznym Bolka i wysyła kryptogram klucza $E_B(K)$ do Bolka
- Bolek deszyfruje kryptogram klucza używając swojego klucza prywatnego, $D_B(E_B(K)) = K$, otrzymując klucz K dla obecnej sesji
- oboje używają klucza K i symetrycznego algorytmu do szyfrowania i deszyfrowania informacji przesyłanych w czasie tej sesji

4.7 Kryptosystem hybrydowy

- Bolek wysyła do Alicji swój klucz publiczny
- Alicja generuje losowy klucz K dla obecnej sesji, szyfruje go kluczem publicznym Bolka i wysyła kryptogram klucza $E_B(K)$ do Bolka
- Bolek deszyfruje kryptogram klucza używając swojego klucza prywatnego, $D_B(E_B(K)) = K$, otrzymując klucz K dla obecnej sesji
- oboje używają klucza K i symetrycznego algorytmu do szyfrowania i deszyfrowania informacji przesyłanych w czasie tej sesji

- Uwagi:
  - algorytmy symetryczne są szybsze niż algorytmy asymetryczne, co ma znaczenie przy przesyłaniu dużej ilości danych
  - jeśli Ewa zdobędzie klucz K, to może go użyć do deszyfrowania jedynie aktualnej sesji, potem już jest bezużyteczny

- Uwagi:
  - algorytmy symetryczne są szybsze niż algorytmy asymetryczne, co ma znaczenie przy przesyłaniu dużej ilości danych
  - jeśli Ewa zdobędzie klucz K, to może go użyć do deszyfrowania jedynie aktualnej sesji, potem już jest bezużyteczny

- Uwagi:
  - algorytmy symetryczne są szybsze niż algorytmy asymetryczne, co ma znaczenie przy przesyłaniu dużej ilości danych
  - jeśli Ewa zdobędzie klucz K, to może go użyć do deszyfrowania jedynie aktualnej sesji, potem już jest bezużyteczny

4.8 Podpis cyfrowy: kryptosystem z kluczem publicznym

- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

4.8 Podpis cyfrowy: kryptosystem z kluczem publicznym

- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

4.8 Podpis cyfrowy: kryptosystem z kluczem publicznym

- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

4.8 Podpis cyfrowy: kryptosystem z kluczem publicznym

- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

- Uwagi:
  - podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
  - podpis nie może być sfałszowany; tylko Alicja zna jej klucz prywatny
  - podpis nie może być przeniesiony do innego dokumentu
  - podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
  - podpis jest niezaprzeczalny;

- Uwagi:
  - podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
  - podpis nie może być sfałszowany; tylko Alicja zna jej klucz prywatny
  - podpis nie może być przeniesiony do innego dokumentu
  - podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
  - podpis jest niezaprzeczalny;

- Uwagi:
  - podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
  - podpis nie może być sfałszowany; tylko Alicja zna jej klucz prywatny
  - podpis nie może być przeniesiony do innego dokumentu
  - podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
  - podpis jest niezaprzeczalny;

- Uwagi:
  - podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
  - podpis nie może być sfałszowany; tylko Alicja zna jej klucz prywatny
  - podpis nie może być przeniesiony do innego dokumentu
  - podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
  - podpis jest niezaprzeczalny;

- Uwagi:
  - podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
  - podpis nie może być sfałszowany; tylko Alicja zna jej klucz prywatny
  - podpis nie może być przeniesiony do innego dokumentu
  - podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
  - podpis jest niezaprzeczalny;

- Uwagi:
  - podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
  - podpis nie może być sfałszowany; tylko Alicja zna jej klucz prywatny
  - podpis nie może być przeniesiony do innego dokumentu
  - podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
  - podpis jest niezaprzeczalny;

4.9 Jednokierunkowe funkcje hashujące (skrótu)

- dla każdego X łatwo jest obliczyć $H(X)$
- $H(X)$ ma taką samą długość dla wszystkich tekstów X
- dla zadanego Y znalezienie takiego X, że $H(X) = Y$ jest praktycznie niemożliwe
- dla zadanego X trudno znaleźć X' takie, że $H(X) = H(X')$

4.9 Jednokierunkowe funkcje hashujące (skrótu)

- dla każdego X łatwo jest obliczyć $H(X)$
- $H(X)$ ma taką samą długość dla wszystkich tekstów X
- dla zadanego Y znalezienie takiego X, że $H(X) = Y$ jest praktycznie niemożliwe
- dla zadanego X trudno znaleźć X' takie, że $H(X) = H(X')$

4.9 Jednokierunkowe funkcje hashujące (skrótu)

- dla każdego X łatwo jest obliczyć $H(X)$
- $H(X)$ ma taką samą długość dla wszystkich tekstów X
- dla zadanego Y znalezienie takiego X, że $H(X) = Y$ jest praktycznie niemożliwe
- dla zadanego X trudno znaleźć X' takie, że $H(X) = H(X')$

4.9 Jednokierunkowe funkcje hashujące (skrótu)

- dla każdego X łatwo jest obliczyć $H(X)$
- $H(X)$ ma taką samą długość dla wszystkich tekstów X
- dla zadanego Y znalezienie takiego X, że $H(X) = Y$ jest praktycznie niemożliwe
- dla zadanego X trudno znaleźć X' takie, że $H(X) = H(X')$

4.9 Jednokierunkowe funkcje hashujące (skrótu)

- dla każdego X łatwo jest obliczyć $H(X)$
- $H(X)$ ma taką samą długość dla wszystkich tekstów X
- dla zadanego Y znalezienie takiego X, że $H(X) = Y$ jest praktycznie niemożliwe
- dla zadanego X trudno znaleźć X' takie, że $H(X) = H(X')$

4.10 Elektroniczny notariusz

- dla danego dokumentu X obliczamy wartość $H(X)$ i publikujemy lub deponujemy u notariusza wartość $H(X)$
- chcąc udowodnić prawdziwość dokumentu X przedstawiamy dokument, obliczamy $H(X)$ i porównujemy z opublikowaną wcześniej wartością

4.10 Elektroniczny notariusz

- dla danego dokumentu X obliczamy wartość $H(X)$ i publikujemy lub deponujemy u notariusza wartość $H(X)$
- chcąc udowodnić prawdziwość dokumentu X przedstawiamy dokument, obliczamy $H(X)$ i porównujemy z opublikowaną wcześniej wartością

4.10 Elektroniczny notariusz

- dla danego dokumentu X obliczamy wartość $H(X)$ i publikujemy lub deponujemy u notariusza wartość $H(X)$
- chcąc udowodnić prawdziwość dokumentu X przedstawiamy dokument, obliczamy $H(X)$ i porównujemy z opublikowaną wcześniej wartością

4.11 Operacja XOR i szyfr Vernama

4.11.1 Operacja XOR czyli dodawanie modulo 2

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 0 &= 1 \\ 1 \oplus 1 &= 0 \end{aligned}$$

- tekst jawny jest ciągiem bitów

  $M = m_1, m_2, \ldots, m_n$

- wybieramy losowy ciąg bitów

  $K = k_1, k_2, \ldots, k_n$, który stanowi klucz

- szyfrowanie polega na wykonaniu operacji xor bit po bicie;

  otrzymujemy w ten sposób losowy ciąg bitów stanowiących

  kryptogram $C = c_1, c_2, \ldots, c_n$, gdzie $c_i = m_i \oplus k_i$

- operacja ta jest odwracalna;

  ponieważ $a \oplus a = 0$ i $a \oplus b \oplus b = a$, zatem

  $c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i$

- tekst jawny jest ciągiem bitów

  $M = m_1, m_2, \ldots, m_n$

- wybieramy losowy ciąg bitów

  $K = k_1, k_2, \ldots, k_n$, który stanowi klucz

- szyfrowanie polega na wykonaniu operacji xor bit po bicie;

  otrzymujemy w ten sposób losowy ciąg bitów stanowiących

  kryptogram $C = c_1, c_2, \ldots, c_n$, gdzie $c_i = m_i \oplus k_i$

- operacja ta jest odwracalna;

  ponieważ $a \oplus a = 0$ i $a \oplus b \oplus b = a$, zatem

  $c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i$

- tekst jawny jest ciągiem bitów

  $M = m_1, m_2, \ldots, m_n$

- wybieramy losowy ciąg bitów

  $K = k_1, k_2, \ldots, k_n$, który stanowi klucz

- szyfrowanie polega na wykonaniu operacji xor bit po bicie;

  otrzymujemy w ten sposób losowy ciąg bitów stanowiących kryptogram $C = c_1, c_2, \ldots, c_n$, gdzie $c_i = m_i \oplus k_i$

- operacja ta jest odwracalna;

  ponieważ $a \oplus a = 0$ i $a \oplus b \oplus b = a$, zatem

  $c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i$

- tekst jawny jest ciągiem bitów

  $M = m_1, m_2, \ldots, m_n$

- wybieramy losowy ciąg bitów

  $K = k_1, k_2, \ldots, k_n$, który stanowi klucz

- szyfrowanie polega na wykonaniu operacji xor bit po bicie;

  otrzymujemy w ten sposób losowy ciąg bitów stanowiących kryptogram $C = c_1, c_2, \ldots, c_n$, gdzie $c_i = m_i \oplus k_i$

- operacja ta jest odwracalna;

  ponieważ $a \oplus a = 0$ i $a \oplus b \oplus b = a$, zatem

  $c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i$

- kryptogram jest losowym ciągiem n bitów

  Jeśli $k_i = m_i$ to $c_i = 0$, w przeciwnym wypadku $c_i = 1$; prawdopodobieństwo, że $c_i = 0$ jest równe $\frac{1}{2}$ niezależnie od wartości m_i, zatem i-ty bit kryptogramu jest losowy

- szyfr ten jest nie do złamania — bezpieczeństwo doskonałe — nie można uzyskać żadnej informacji o tekście jawnym bez znajomości klucza

  Ponieważ $c_i = m_i \oplus k_i$ implikuje $k_i = m_i \oplus c_i$, a kryptogram $c_1, c_2, \ldots, c_n$ odpowiada każdemu możliwemu tekstowi jawnemu z takim samym prawdopodobieństwem, to na podstawie samego kryptogramu nie wiemy nic o tekście jawnym

- kryptogram jest losowym ciągiem n bitów

  Jeśli $k_i = m_i$ to $c_i = 0$, w przeciwnym wypadku $c_i = 1$; prawdopodobieństwo, że $c_i = 0$ jest równe $\frac{1}{2}$ niezależnie od wartości m_i, zatem i-ty bit kryptogramu jest losowy

- szyfr ten jest nie do złamania — bezpieczeństwo doskonałe — nie można uzyskać żadnej informacji o tekście jawnym bez znajomości klucza

  Ponieważ $c_i = m_i \oplus k_i$ implikuje $k_i = m_i \oplus c_i$, a kryptogram $c_1, c_2, \ldots, c_n$ odpowiada każdemu możliwemu tekstowi jawnemu z takim samym prawdopodobieństwem, to na podstawie samego kryptogramu nie wiemy nic o tekście jawnym

- Problemy:
  - klucz musi być wcześniej uzgodniony przez Alicję i Bolka
  - klucz musi być wybrany naprawdę losowo, co nie jest łatwe
  - klucz musi być przechowywany w bezpieczny sposób
  - klucz musi być co najmniej tak długi jak szyfrowany tekst

- Problemy:
  - klucz musi być wcześniej uzgodniony przez Alicję i Bolka
  - klucz musi być wybrany naprawdę losowo, co nie jest łatwe
  - klucz musi być przechowywany w bezpieczny sposób
  - klucz musi być co najmniej tak długi jak szyfrowany tekst

- Problemy:
  - klucz musi być wcześniej uzgodniony przez Alicję i Bolka
  - klucz musi być wybrany naprawdę losowo, co nie jest łatwe
  - klucz musi być przechowywany w bezpieczny sposób
  - klucz musi być co najmniej tak długi jak szyfrowany tekst

- Problemy:
  - klucz musi być wcześniej uzgodniony przez Alicję i Bolka
  - klucz musi być wybrany naprawdę losowo, co nie jest łatwe
  - klucz musi być przechowywany w bezpieczny sposób
  - klucz musi być co najmniej tak długi jak szyfrowany tekst

- Problemy:
  - klucz musi być wcześniej uzgodniony przez Alicję i Bolka
  - klucz musi być wybrany naprawdę losowo, co nie jest łatwe
  - klucz musi być przechowywany w bezpieczny sposób
  - klucz musi być co najmniej tak długi jak szyfrowany tekst

- Problemy:
  - klucz musi być wcześniej uzgodniony przez Alicję i Bolka
  - klucz musi być wybrany naprawdę losowo, co nie jest łatwe
  - klucz musi być przechowywany w bezpieczny sposób
  - klucz musi być co najmniej tak długi jak szyfrowany tekst

- Przykład:

tekst jawny	$\Longrightarrow$	S	Z	Y	F	R
binarnie	$\Longrightarrow$	01010011	01011010	01011001	01000110	01010010
klucz	$\Longrightarrow$	01110010	01010101	11011100	10110011	00101011
kryptogram	$\Longrightarrow$	00100001	00001111	10000101	11110101	01111001