

Stefan Sokołowski

KRYPTOGRAFIA

wykład 4

Inst. Informatyki Stosowanej, ANS

Elbląg, 2026/2027

Przypomnienie — arytmetyka „modulo”

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \iff^{\text{def}} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1) \quad \text{równoważne modulo } n$$

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1) \quad \text{równoważne modulo } n$$

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$(657 \cdot 9876 + 23 \cdot 177) \cdot 77777 \equiv_9$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$\begin{aligned} & (657 \cdot 9876 + 23 \cdot 177) \cdot 77777 \\ & \equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35 \end{aligned}$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1) \quad \text{równoważne modulo } n$$

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$\begin{aligned} & (657 \cdot 9876 + 23 \cdot 177) \cdot 77777 \\ & \equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35 \\ & \equiv_9 (9 \cdot 3 + 5 \cdot 6) \cdot 8 \end{aligned}$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$(657 \cdot 9876 + 23 \cdot 177) \cdot 77777$$

$$\equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35$$

$$\equiv_9 (9 \cdot 3 + 5 \cdot 6) \cdot 8 \equiv_9 (0 + 30) \cdot 8$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1)$$

równoważne
modulo n

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$(657 \cdot 9876 + 23 \cdot 177) \cdot 77777$$

$$\equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35$$

$$\equiv_9 (9 \cdot 3 + 5 \cdot 6) \cdot 8 \equiv_9 (0 + 30) \cdot 8$$

$$\equiv_9 3 \cdot 8$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1) \quad \text{równoważne modulo } n$$

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$\begin{aligned} & (657 \cdot 9876 + 23 \cdot 177) \cdot 77777 \\ & \equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35 \\ & \equiv_9 (9 \cdot 3 + 5 \cdot 6) \cdot 8 \equiv_9 (0 + 30) \cdot 8 \\ & \equiv_9 3 \cdot 8 \equiv_9 24 \end{aligned}$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1) \quad \text{równoważne modulo } n$$

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$\begin{aligned} & (657 \cdot 9876 + 23 \cdot 177) \cdot 77777 \\ & \equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35 \\ & \equiv_9 (9 \cdot 3 + 5 \cdot 6) \cdot 8 \equiv_9 (0 + 30) \cdot 8 \\ & \equiv_9 3 \cdot 8 \equiv_9 24 \equiv_9 6 \end{aligned}$$

Przypomnienie — arytmetyka „modulo”

Niech $n \in \mathbb{N}_{\geq 2}$. Utożsamiamy liczby, dające taką samą resztę w dzieleniu przez n :

$$k_0 \equiv_n k_1 \stackrel{\text{def}}{\iff} n \mid (k_0 - k_1) \quad \text{równoważne modulo } n$$

Przykład:

$$11 \equiv_{10} 1 \equiv_{10} -9 \not\equiv_{10} -1$$

reszta z dzielenia -9 przez 10 jest 1
inaczej niż w językach programowania!

Ta relacja jest *kongruencją* ze względu na dodawanie, odejmowanie i mnożenie:

jeśli $k_0 \equiv_n k_1$ i $\ell_0 \equiv_n \ell_1$,

to $k_0 + \ell_0 \equiv_n k_1 + \ell_1$

$$k_0 - \ell_0 \equiv_n k_1 - \ell_1$$

$$k_0 \cdot \ell_0 \equiv_n k_1 \cdot \ell_1$$

Przykład:

$$\begin{aligned} & (657 \cdot 9876 + 23 \cdot 177) \cdot 77777 \\ & \equiv_9 (18 \cdot 30 + 5 \cdot 15) \cdot 35 \\ & \equiv_9 (9 \cdot 3 + 5 \cdot 6) \cdot 8 \equiv_9 (0 + 30) \cdot 8 \\ & \equiv_9 3 \cdot 8 \equiv_9 24 \equiv_9 6 \end{aligned}$$

Uwaga:

Równoważność modulo nie jest kongruencją ze względu na dzielenie (patrz dalej).

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n**

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k$$

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k$$

lemat Bézout

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k \equiv_n y \cdot k$$

lemat Bézout

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k \equiv_n y \cdot k$$

więc y jest odwrotnością k modulo n . lemat Bézout

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k \equiv_n y \cdot k$$

więc y jest odwrotnością k modulo n . lemat Bézout

Wniosek:

Dzielić modulo n można przez liczby względnie pierwsze z n i tylko przez nie.

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k \equiv_n y \cdot k$$

więc y jest odwrotnością k modulo n . lemat Bézout

Wniosek:

Dzielić modulo n można przez liczby względnie pierwsze z n i tylko przez nie. Jeśli n jest liczbą pierwszą, to można dzielić przez wszystko z wyjątkiem wielokrotności n (które są $\equiv_n 0$).

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k \equiv_n y \cdot k$$

więc y jest odwrotnością k modulo n . lemat Bézout

Wniosek:

*Dzielić modulo n można przez liczby względnie pierwsze z n i tylko przez nie.
Jeśli n jest liczbą pierwszą, to można dzielić przez wszystko z wyjątkiem wielokrotności n (które są $\equiv_n 0$).*

Twierdzenie:

$$\text{Jeśli } \left\{ \begin{array}{l} k_0 \cdot \ell_0 \equiv_n 1 \\ k_1 \cdot \ell_1 \equiv_n 1 \\ k_0 \equiv_n k_1 \end{array} \right\} \text{ to } \ell_0 \equiv_n \ell_1 .$$

Przypomnienie — dzielenie modulo

Jeśli $\text{nwd}(n, k) > 1$, czyli n i k mają wspólny czynnik większy niż 1, to **nie istnieje odwrotność liczby k modulo n** , czyli nie ma takiego ℓ , że $k \cdot \ell \equiv_n 1$, więc dzielenie modulo n przez k **nie jest wykonalne**.

Jeśli $\text{nwd}(n, k) = 1$, to istnieją $x, y \in \mathbb{Z}$ t.ż.

$$1 = x \cdot n + y \cdot k \equiv_n y \cdot k$$

więc y jest odwrotnością k modulo n . — lemat Bézout

Wniosek:

Dzielić modulo n można przez liczby względnie pierwsze z n i tylko przez nie. Jeśli n jest liczbą pierwszą, to można dzielić przez wszystko z wyjątkiem wielokrotności n (które są $\equiv_n 0$).

Twierdzenie:

$$\text{Jeśli } \left\{ \begin{array}{l} k_0 \cdot \ell_0 \equiv_n 1 \\ k_1 \cdot \ell_1 \equiv_n 1 \\ k_0 \equiv_n k_1 \end{array} \right\} \text{ to } \ell_0 \equiv_n \ell_1 .$$

Wniosek:

Jeśli dwie liczby są równe modulo n , to ich odwrotności (o ile istnieją) są również równe modulo n .

Przypomnienie — własności arytmetyki modulo

Twierdzenie:

Jeśli $0 \leq a < n$, $0 \leq b < n$ i $a \equiv_n b$, to $a = b$.

Przypomnienie — własności arytmetyki modulo

Twierdzenie:

Jeśli $0 \leq a < n$, $0 \leq b < n$ i $a \equiv_n b$, to $a = b$.

Twierdzenie:

Jeśli $\text{nwd}(p, q) = 1$ (liczby względnie pierwsze), to

$$a \equiv_{p \cdot q} b \iff \begin{cases} a \equiv_p b \\ \wedge \\ a \equiv_q b \end{cases}$$

Przypomnienie — własności arytmetyki modulo

Twierdzenie:

Jeśli $0 \leq a < n$, $0 \leq b < n$ i $a \equiv_n b$, to $a = b$.

Twierdzenie:

Jeśli $\text{nwd}(p, q) = 1$ (liczby względnie pierwsze), to

$$a \equiv_{p \cdot q} b \iff \begin{cases} a \equiv_p b \\ \wedge \\ a \equiv_q b \end{cases}$$

Twierdzenie: (małe twierdzenie Fermata)

Jeśli p jest liczbą pierwszą, to $a^p \equiv_p a$ dla dowolnego $a \in \mathbb{Z}$.

Przypomnienie — własności arytmetyki modulo

Twierdzenie:

Jeśli $0 \leq a < n$, $0 \leq b < n$ i $a \equiv_n b$, to $a = b$.

Twierdzenie:

Jeśli $\text{nwd}(p, q) = 1$ (liczby względnie pierwsze), to

$$a \equiv_{p \cdot q} b \iff \begin{cases} a \equiv_p b \\ \wedge \\ a \equiv_q b \end{cases}$$

Twierdzenie: (małe twierdzenie Fermata)

Jeśli p jest liczbą pierwszą, to $a^p \equiv_p a$ dla dowolnego $a \in \mathbb{Z}$.

Wniosek:

Jeśli p jest liczbą pierwszą, to $a^{p-1} \equiv_p 1$ dla dowolnego $a \in \mathbb{Z}$ t.ż. $p \nmid a$.

Szyfrowanie asymetryczne RSA



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$;
- wybiera liczbę e , t.ż.
 $1 < e < (p - 1) \cdot (q - 1)$
oraz
 $\text{nwd}(e, (p - 1) \cdot (q - 1)) = 1$



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$;
- wybiera liczbę e , t.ż.
 $1 < e < (p-1) \cdot (q-1)$
oraz
 $\text{nwd}(e, (p-1) \cdot (q-1)) = 1$;
- znajduje odwrotność d liczby e modulo $(p-1) \cdot (q-1)$; czyli
 $e \cdot d \equiv_{(p-1)(q-1)} 1$



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$;
- wybiera liczbę e , t.ż.
 $1 < e < (p-1) \cdot (q-1)$
oraz
 $\text{nwd}(e, (p-1) \cdot (q-1)) = 1$;
- znajduje odwrotność d liczby e modulo $(p-1) \cdot (q-1)$; czyli
 $e \cdot d \equiv_{(p-1)(q-1)} 1$;
- ogłasza (n, e) jako klucz **publiczny**



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$;
- wybiera liczbę e , t.ż.
 $1 < e < (p-1) \cdot (q-1)$
oraz
 $\text{nwd}(e, (p-1) \cdot (q-1)) = 1$;
- znajduje odwrotność d liczby e modulo $(p-1) \cdot (q-1)$; czyli
 $e \cdot d \equiv_{(p-1)(q-1)} 1$;
- ogłasza (n, e) jako klucz **publiczny**: bloki wiadomości (liczby mniejsze niż n) do niego należy szyfrować tak:
 $M \rightarrow M^e \bmod n$



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$;
- wybiera liczbę e , t.ż.
 $1 < e < (p-1) \cdot (q-1)$
oraz
 $\text{nwd}(e, (p-1) \cdot (q-1)) = 1$;
- znajduje odwrotność d liczby e modulo $(p-1) \cdot (q-1)$; czyli
 $e \cdot d \equiv_{(p-1)(q-1)} 1$;
- ogłasza (n, e) jako klucz **publiczny**: bloki wiadomości (liczby mniejsze niż n) do niego należy szyfrować tak:
 $M \rightarrow M^e \bmod n$;
- zachowuje w tajemnicy (n, d) — klucz **prywatny**



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Właściciel szyfru:

- wybiera dwie duże różne liczby pierwsze p i q ;
niech $n = p \cdot q$;
- wybiera liczbę e , t.ż.
 $1 < e < (p-1) \cdot (q-1)$
oraz
 $\text{nwd}(e, (p-1) \cdot (q-1)) = 1$;
- znajduje odwrotność d liczby e modulo $(p-1) \cdot (q-1)$; czyli
 $e \cdot d \equiv_{(p-1)(q-1)} 1$;
- ogłasza (n, e) jako klucz **publiczny**: bloki wiadomości (liczby mniejsze niż n) do niego należy szyfrować tak:
 $M \rightarrow M^e \bmod n$;
- zachowuje w tajemnicy (n, d) — klucz **prywatny**: otrzymane zaszyfrowane wiadomości będzie odszyfrowywać tak:
 $C \rightarrow C^d \bmod n$.



Ron
Rivest



Adi
Shamir



Leonard
Adleman

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$(M^e)^d = M^{ed}$$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$(M^e)^d = M^{ed} = M \cdot M^{ed-1}$$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$(M^e)^d = M^{ed} = M \cdot M^{ed-1} = M \cdot M^{k(p-1)}$$

$ed \equiv_{(p-1)(q-1)} 1$
więc $ed - 1$ dzieli się
przez $p-1$ i przez $q-1$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$\begin{aligned} (M^e)^d &= M^{ed} = M \cdot M^{ed-1} = M \cdot M^{k(p-1)} \\ &= M \cdot (M^{p-1})^k \end{aligned}$$

$ed \equiv_{(p-1)(q-1)} 1$
więc $ed - 1$ dzieli się
przez $p-1$ i przez $q-1$

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$\begin{aligned} (M^e)^d &= M^{ed} = M \cdot M^{ed-1} = M \cdot M^{k(p-1)} \\ &= M \cdot (M^{p-1})^k \equiv_p M \cdot 1^k \end{aligned}$$

$ed \equiv_{(p-1)(q-1)} 1$
więc $ed - 1$ dzieli się
przez $p-1$ i przez $q-1$

wniosek z
małego tw. Fermata

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$\begin{aligned} (M^e)^d &= M^{ed} = M \cdot M^{ed-1} = M \cdot M^{k(p-1)} \\ &= M \cdot (M^{p-1})^k \equiv_p M \cdot 1^k = M \end{aligned}$$

$ed \equiv_{(p-1)(q-1)} 1$
więc $ed - 1$ dzieli się
przez $p-1$ i przez $q-1$

wniosek z
małego tw. Fermata

Szyfrowanie asymetryczne RSA

Twierdzenie:

Przy tych założeniach $(M^e)^d \equiv_n M$; czyli zaszyfrowanie M kluczem publicznym a następnie odszyfrowanie prywatnym prowadzi znowu do M .

Dowód:

Ponieważ $n = p \cdot q$ i $\text{nwd}(p, q) = 1$, wystarczy dowieść osobno

$$(M^e)^d \equiv_p M \quad \text{i} \quad (M^e)^d \equiv_q M .$$

Przyp. $M \equiv_p 0$:

M jest wielokrotnością p , więc $(M^e)^d$ jest wielokrotnością p ,
więc $(M^e)^d \equiv_p 0 \equiv_p M$.

Przyp. $M \not\equiv_p 0$:

$$\begin{aligned} (M^e)^d &= M^{ed} = M \cdot M^{ed-1} = M \cdot M^{k(p-1)} \\ &= M \cdot (M^{p-1})^k \equiv_p M \cdot 1^k = M \end{aligned}$$

$(M^e)^d \equiv_q M$ tak samo.

□

wniosek z
małego tw. Fermata

$ed \equiv_{(p-1)(q-1)} 1$
więc $ed - 1$ dzieli się
przez $p-1$ i przez $q-1$

Szyfrowanie asymetryczne RSA — przykład

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200 \\ \text{z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$e = 4321$ — wzgl. pierwszy z 34200
z alg. Euklidesa:

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

więc $4321 \cdot 2881 \equiv_{34200} 1$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Nadawca:

Klucz jawny: $(34571, 4321)$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Nadawca:

Klucz jawny: $(34571, 4321)$

$$M = 12345$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Nadawca:

Klucz jawny: $(34571, 4321)$

$$M = 12345$$

$$12345^{4321} \equiv_{34571} 17413$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Nadawca:

Klucz jawny: $(34571, 4321)$

$$M = 12345$$

$$12345^{4321} \equiv_{34571} 17413$$

Odbiorca:

Klucz tajny: $(34571, 2881)$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Nadawca:

Klucz jawny: $(34571, 4321)$

$$M = 12345$$

$$12345^{4321} \equiv_{34571} 17413$$

Odbiorca:

Klucz tajny: $(34571, 2881)$

$$C = 17413$$

Szyfrowanie asymetryczne RSA — przykład

Liczby pierwsze:

$$p = 181 \text{ i } q = 191$$

$$n = p \cdot q = 34571$$

$$(p-1) \cdot (q-1) = 34200$$

Wybór kluczy:

$$e = 4321 \text{ — wzgl.pierwszy z } 34200$$

$$d = 2881 \text{ z alg. Euklidesa:}$$

$$34200 \cdot (-364) + 4321 \cdot 2881 = 1$$

$$\text{więc } 4321 \cdot 2881 \equiv_{34200} 1$$

Nadawca:

Klucz jawny: $(34571, 4321)$

$$M = 12345$$

$$12345^{4321} \equiv_{34571} 17413$$

Odbiorca:

Klucz tajny: $(34571, 2881)$

$$C = 17413$$

$$17413^{2881} \equiv_{34571} 12345$$

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co wlamywalicz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
mógłby obliczyć q z (1) i (4)

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p)

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
 mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p);
 a następnie z (2) i (3) obliczyć d .

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
 mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p);
 a następnie z (2) i (3) obliczyć d , czyli odwrotność e modulo $(p-1) \cdot (q-1)$.

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
 mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p);
 a następnie z (2) i (3) obliczyć d , czyli odwrotność e modulo $(p-1) \cdot (q-1)$.

Ale żeby znać p trzeba rozłożyć na czynniki n .

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
 mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p);
 a następnie z (2) i (3) obliczyć d , czyli odwrotność e modulo $(p-1) \cdot (q-1)$.

Ale żeby znać p trzeba rozłożyć na czynniki n .

Nie ma znanych algorytmów pozwalających na dzisiejszych komputerach rozłożyć na czynniki w rozsądnym czasie liczbę ponad 2000-bitową (ok. 620 cyfr dziesiętnych).

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
 mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p);
 a następnie z (2) i (3) obliczyć d , czyli odwrotność e modulo $(p-1) \cdot (q-1)$.

Ale żeby znać p trzeba rozłożyć na czynniki n .

Nie ma znanych algorytmów pozwalających na dzisiejszych komputerach rozłożyć na czynniki w rozsądnym czasie liczbę ponad 2000-bitową (ok. 620 cyfr dziesiętnych).

Pomnożyć liczby pierwsze p i q (nawet olbrzymie) — to łatwe.

Szyfrowanie asymetryczne RSA — bezpieczeństwo

Czy szyfrowanie RSA jest bezpieczne? Co włamywacz wie, a czego potrzebuje?

	potrzebuje	zna	wie
(1)	n	tak	
(2)	d	nie	$e \cdot d \equiv_{(p-1)(q-1)} 1$
(3)	e	tak	
(4)	$p-1, q-1$	nie	$n = p \cdot q$

Gdyby włamywacz znał p ,
 mógłby obliczyć q z (1) i (4) (albo gdyby znał q , mógłby obliczyć p);
 a następnie z (2) i (3) obliczyć d , czyli odwrotność e modulo $(p-1) \cdot (q-1)$.

Ale żeby znać p trzeba rozłożyć na czynniki n .

Nie ma znanych algorytmów pozwalających na dzisiejszych komputerach rozłożyć na czynniki w rozsądnym czasie liczbę ponad 2000-bitową (ok. 620 cyfr dziesiętnych).

**Pomnożyć liczby pierwsze p i q (nawet olbrzymie) — to łatwe.
 Rozłożyć ich iloczyn na czynniki — to bardzo trudne.**

Szyfrowanie asymetryczne — podpis cyfrowy

Szyfrowanie asymetryczne — podpis cyfrowy

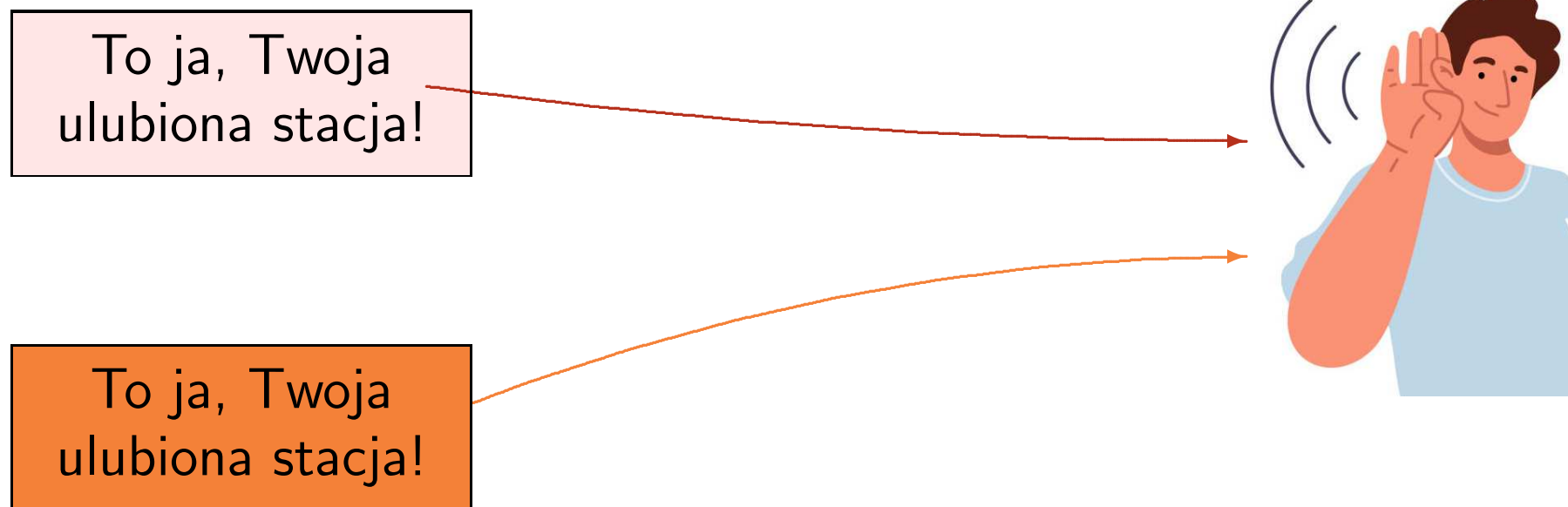


Szyfrowanie asymetryczne — podpis cyfrowy

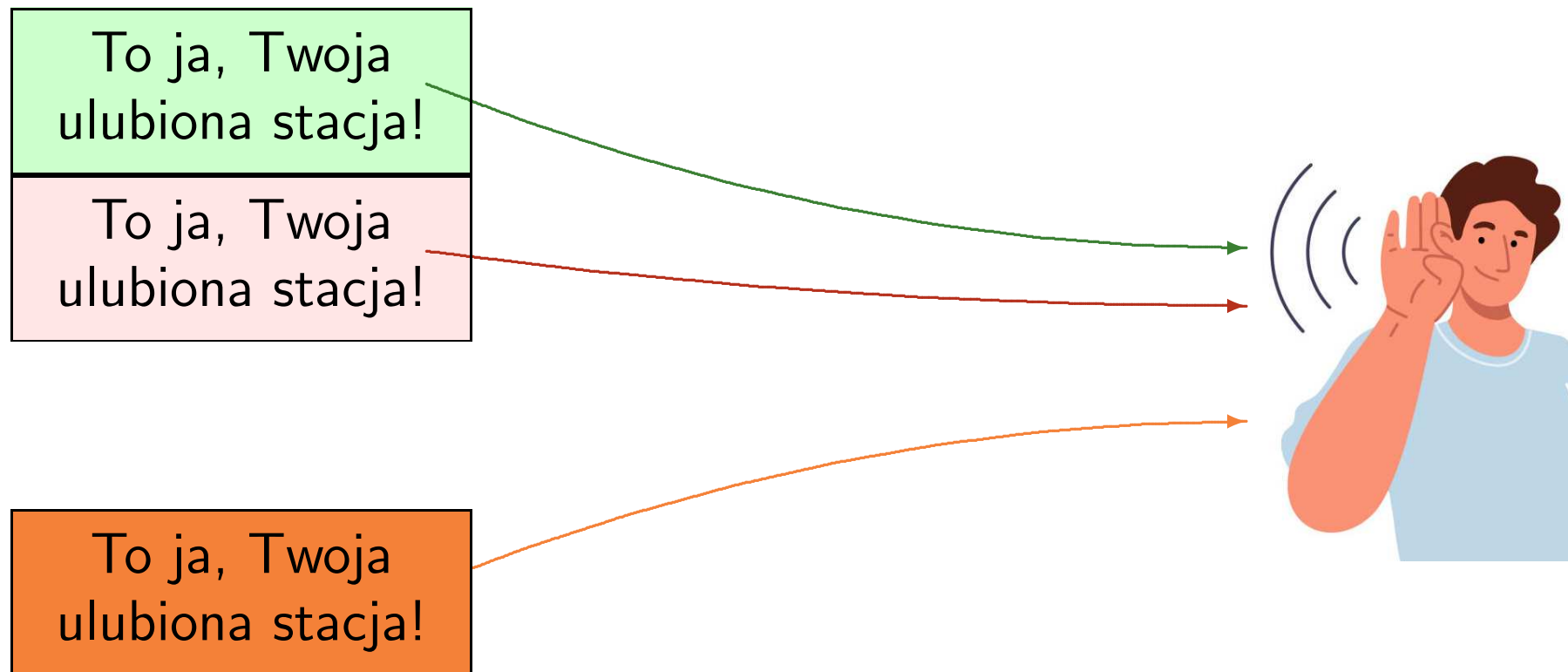
To ja, Twoja
ulubiona stacja!



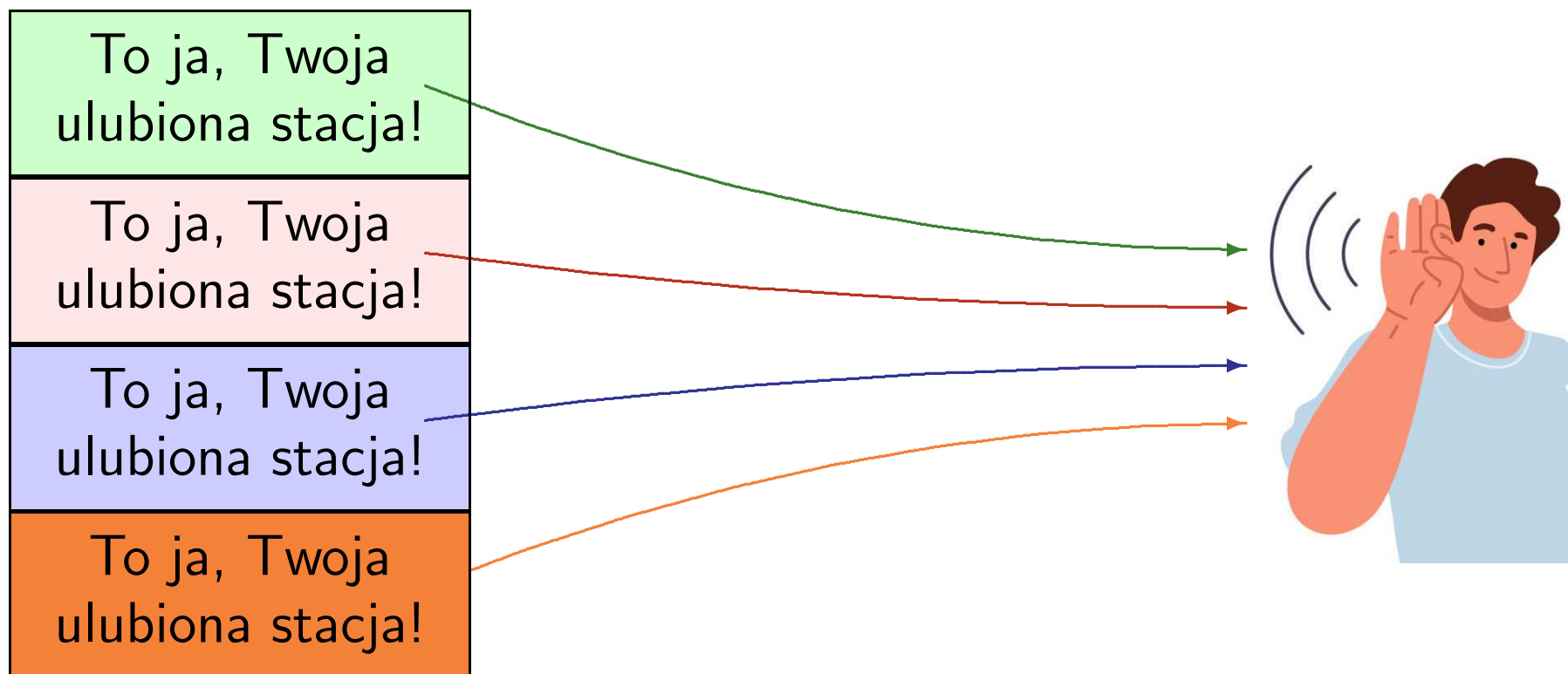
Szyfrowanie asymetryczne — podpis cyfrowy



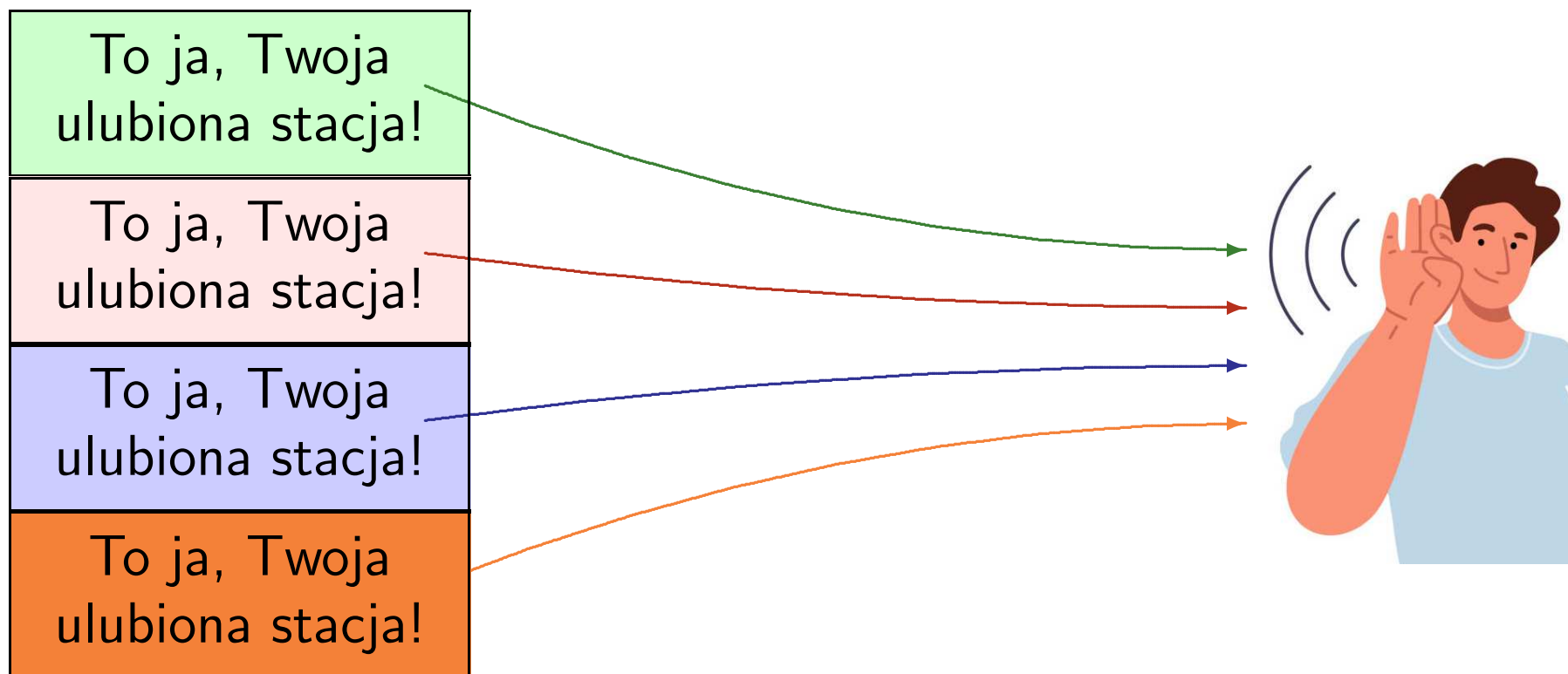
Szyfrowanie asymetryczne — podpis cyfrowy



Szyfrowanie asymetryczne — podpis cyfrowy

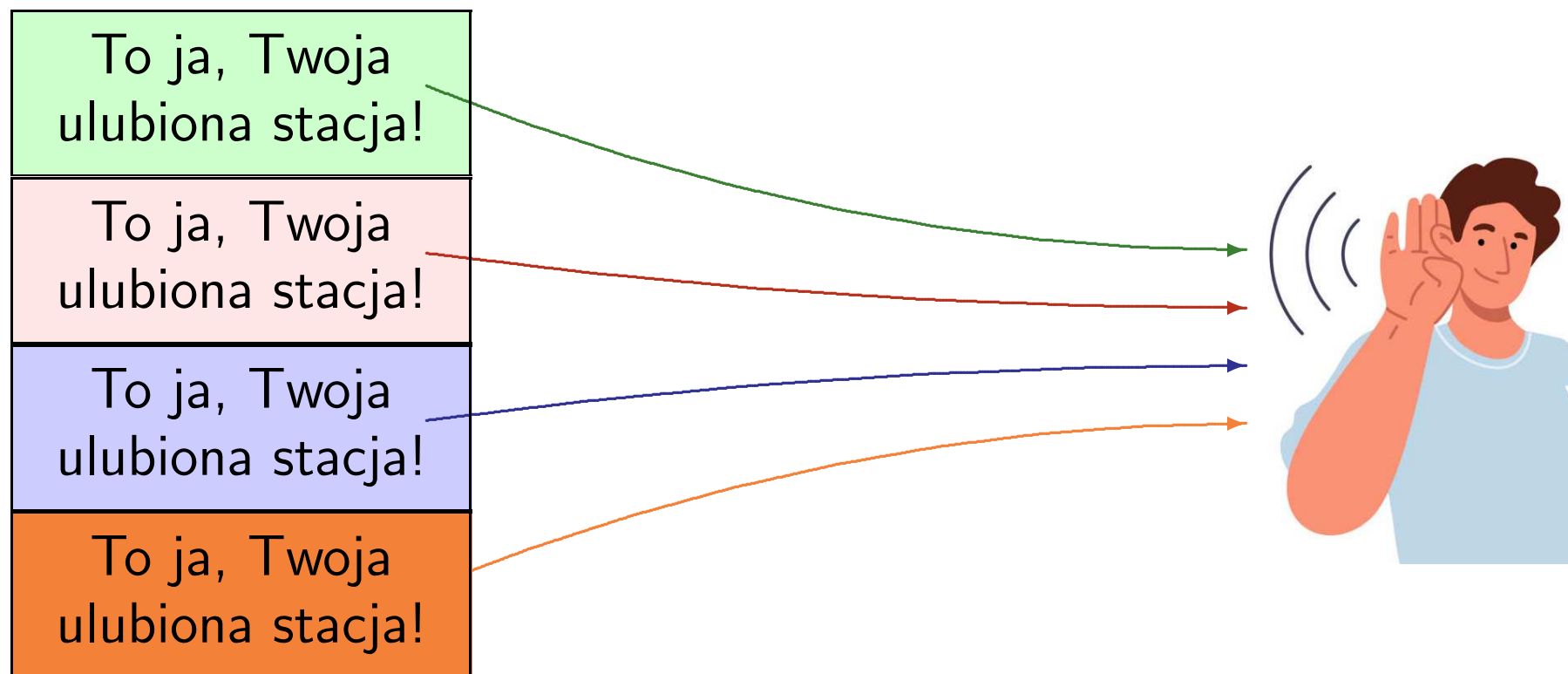


Szyfrowanie asymetryczne — podpis cyfrowy



Różni nadawcy podszywają się pod „ulubionego”.

Szyfrowanie asymetryczne — podpis cyfrowy



Różni nadawcy podszywają się pod „ulubionego”.
Jak się przekonać, który z nich to ten **prawdziwy**?

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa;
- **integralności** — żeby dało się wykryć przeróbki dokonane już po „podpisaniu”.

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa;
- **integralności** — żeby dało się wykryć przeróbki dokonane już po „podpisaniu”.

Jak to osiągnąć?

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa;
- **integralności** — żeby dało się wykryć przeróbki dokonane już po „podpisaniu”.

Jak to osiągnąć?

Uprawniony nadawca ogłasza **klucz publiczny** K_d .

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa;
- **integralności** — żeby dało się wykryć przeróbki dokonane już po „podpisaniu”.

Jak to osiągnąć?

Uprawniony nadawca ogłasza **klucz publiczny** K_d .

Następnie wysyła wiadomości zaszyfrowane **kluczem prywatnym** K_e .

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa;
- **integralności** — żeby dało się wykryć przeróbki dokonane już po „podpisaniu”.

Jak to osiągnąć?

Uprawniony nadawca ogłasza **klucz publiczny** K_d .

Następnie wysyła wiadomości zaszyfrowane **kluczem prywatnym** K_e .

Jeśli (znany odbiorcy) K_d odszyfrowuje wiadomość, to musiała pochodzić od uprawnionego nadawcy

Szyfrowanie asymetryczne — podpis cyfrowy

Podpis cyfrowy — przekształcenie ew. uzupełnienie dokumentu, dające odbiorcy pewność co do:

- **autentyczności** — żeby wiedział, że przysłał ten, kto miał przysłać;
- **niezaprzeczalności** — żeby nadawca nie mógł potem wyprzeć się autorstwa;
- **integralności** — żeby dało się wykryć przeróbki dokonane już po „podpisaniu”.

Jak to osiągnąć?

Uprawniony nadawca ogłasza **klucz publiczny** K_d .

Następnie wysyła wiadomości zaszyfrowane **kluczem prywatnym** K_e .

Jeśli (znany odbiorcy) K_d odszyfrowuje wiadomość, to musiała pochodzić od uprawnionego nadawcy, bo nikt inny nie znał K_e .

Szyfrowanie asymetryczne — poker w pamięci

Poker w pamięci



Szyfrowanie asymetryczne — poker w pamięci

Poker w pamięci



Cel: zorganizować grę w pokera między Anią i Bolkiem

Szyfrowanie asymetryczne — poker w pamięci

Poker w pamięci



Cel: zorganizować grę w pokera między Anią i Bolkiem tak, żeby

- toczyła się **zdalnie** (np. przez telefon)

Szyfrowanie asymetryczne — poker w pamięci

Poker w pamięci



Cel: zorganizować grę w pokera między Anią i Bolkiem tak, żeby

- toczyła się **zdalnie** (np. przez telefon);
- bez żadnego arbitra (tylko ich dwoje)

Szyfrowanie asymetryczne — poker w pamięci

Poker w pamięci



Cel: zorganizować grę w pokera między Anią i Bolkiem tak, żeby

- toczyła się **zdalnie** (np. przez telefon);
- bez żadnego arbitra (tylko ich dwoje);
- żadne z nich nie mogło skutecznie oszukiwać.

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi; Bolek po odkodowaniu wie, co dostał:

$$D_B(E_B(M_i)) = M_i$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi; Bolek po odkodowaniu wie, co dostał:

$$D_B(E_B(M_i)) = M_i ;$$

3. Ania wybiera kolejne 5 kart, koduje je swoim E_A i wysyła do Bolka:

$$E_A(E_B(M_6)), \dots, E_A(E_B(M_{10}))$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi; Bolek po odkodowaniu wie, co dostał:

$$D_B(E_B(M_i)) = M_i ;$$

3. Ania wybiera kolejne 5 kart, koduje je swoim E_A i wysyła do Bolka:

$$E_A(E_B(M_6)), \dots, E_A(E_B(M_{10})) ;$$

4. Bolek odkodowuje je swoim D_B i wysyła do Ani:

$$D_B(E_A(E_B(M_i)))$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi; Bolek po odkodowaniu wie, co dostał:

$$D_B(E_B(M_i)) = M_i ;$$

3. Ania wybiera kolejne 5 kart, koduje je swoim E_A i wysyła do Bolka:

$$E_A(E_B(M_6)), \dots, E_A(E_B(M_{10})) ;$$

4. Bolek odkodowuje je swoim D_B i wysyła do Ani:

$$D_B(\underline{E_A(E_B(M_i))}) = D_B(\underline{E_B(E_A(M_i))})$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi; Bolek po odkodowaniu wie, co dostał:

$$D_B(E_B(M_i)) = M_i ;$$

3. Ania wybiera kolejne 5 kart, koduje je swoim E_A i wysyła do Bolka:

$$E_A(E_B(M_6)), \dots, E_A(E_B(M_{10})) ;$$

4. Bolek odkodowuje je swoim D_B i wysyła do Ani:

$$D_B(\underline{E_A(E_B(M_i))}) = D_B(\underline{E_B(E_A(M_i))}) = E_A(M_i)$$

Szyfrowanie asymetryczne — poker w pamięci

Ania:

klucz jawny E_A

klucz tajny D_A

$$D_A(E_A(M)) = M$$

Bolek:

klucz jawny E_B

klucz tajny D_B

$$D_B(E_B(M)) = M$$

symetria:

$$E_B(E_A(M)) = E_A(E_B(M))$$

Rozdawanie kart:

1. Bolek koduje całą talię kluczem E_B i wysyła do Ani;
2. Ania wybiera 5 losowych kart $E_B(M_1), \dots, E_B(M_5)$ (nie znając D_B , nie wie, co to za karty) i odsyła je Bolkowi; Bolek po odkodowaniu wie, co dostał:

$$D_B(E_B(M_i)) = M_i ;$$

3. Ania wybiera kolejne 5 kart, koduje je swoim E_A i wysyła do Bolka:

$$E_A(E_B(M_6)), \dots, E_A(E_B(M_{10})) ;$$

4. Bolek odkodowuje je swoim D_B i wysyła do Ani:

$$D_B(\underline{E_A(E_B(M_i))}) = D_B(\underline{E_B(E_A(M_i))}) = E_A(M_i) ;$$

5. Ania odkodowuje je przez D_A i wie, co dostała:

$$D_A(E_A(M_i)) = M_i .$$

Szyfrowanie asymetryczne — Diffie-Hellman

**Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał**



Whitfield
Diffie

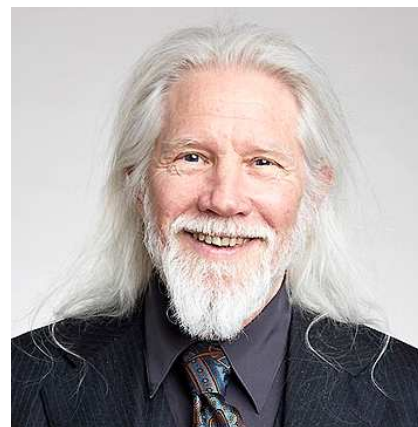


Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	



Whitfield
Diffie



Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$		duża $b \in \mathbb{N}$



Whitfield
Diffie



Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$



Whitfield
Diffie



Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$



Whitfield
Diffie

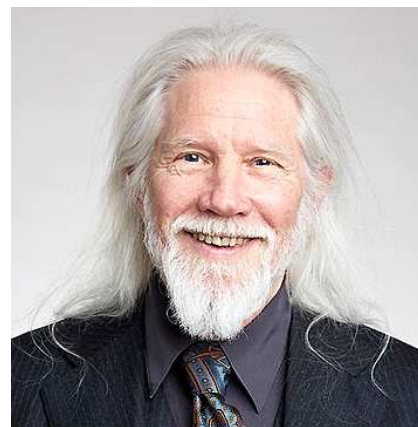


Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
	B	A



Whitfield
Diffie



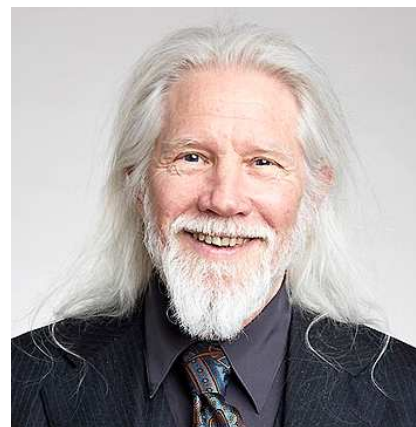
Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of public values A and B between Ania and Bolek. A red arrow points from A in the Bolek column to A in the Ania column. A green arrow points from B in the Ania column to B in the Bolek column.



Whitfield
Diffie



Martin
Hellman

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in Bolek's row to A in the bottom row. A green arrow points from B in Ania's row to B in the bottom row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$K_A \equiv_n B^a$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in the third row to A in the fourth row. A green arrow points from B in the third row to B in the fourth row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

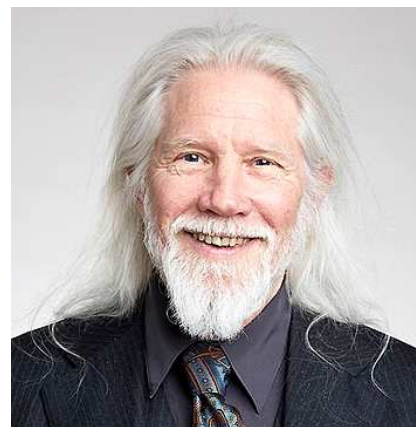
$$K_A \equiv_n B^a \equiv_n (g^b)^a$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in the third row to A in the fourth row. A green arrow points from B in the third row to B in the fourth row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

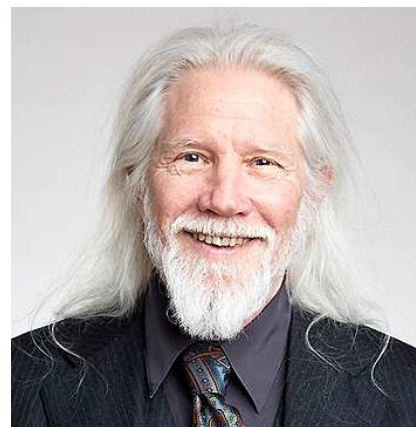
$$K_A \equiv_n B^a \equiv_n (g^b)^a = g^{ba}$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in Bolek's row to A in the 'jawne' column. A green arrow points from B in Ania's row to B in the 'jawne' column.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$K_A \equiv_n B^a \equiv_n (g^b)^a = g^{ba} = g^{ab}$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in the third row to A in the fourth row. A green arrow points from B in the third row to B in the fourth row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$K_A \equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\ = g^{ab} = (g^a)^b$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of public values A and B between Ania and Bolek. A red arrow points from A in the Bolek column to the B in the Ania column. A green arrow points from B in the Ania column to the A in the Bolek column.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b
 \end{aligned}$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in the Bolek column to A in the Ania column. A green arrow points from B in the Ania column to B in the Bolek column.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in Ania's row to A in Bolek's row. A green arrow points from B in Bolek's row to B in Ania's row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

więc Ania i Bolek dysponują tym
samym kluczem $K = K_A = K_B$.

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in the 'Ania' column to A in the 'Bolek' column. A green arrow points from B in the 'Bolek' column to B in the 'Ania' column.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

więc Ania i Bolek dysponują tym
samym kluczem $K = K_A = K_B$.

Ew. włamywacz zna A (oraz B)

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in Bolek's row to A in Ania's row. A green arrow points from B in Ania's row to B in Bolek's row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

więc Ania i Bolek dysponują tym
samym kluczem $K = K_A = K_B$.

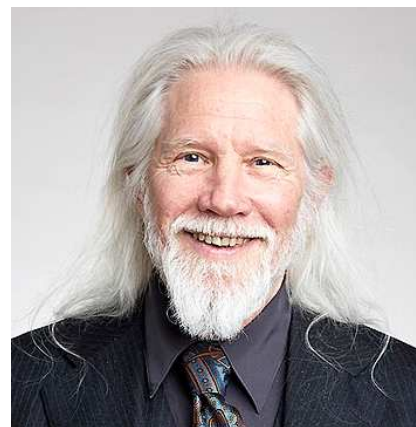
Ew. włamywacz zna A (oraz B) ale nie zna b (ani a)

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in Ania's row to A in Bolek's row. A green arrow points from B in Bolek's row to B in Ania's row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

więc Ania i Bolek dysponują tym
samym kluczem $K = K_A = K_B$.

Ew. włamywacz zna A (oraz B) ale nie zna b (ani a) — nie wie, do jakiej potęgi podnieść A (ew. B), żeby otrzymać klucz.

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in the 'Ania' column to A in the 'Bolek' column. A green arrow points from B in the 'Bolek' column to B in the 'Ania' column.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

więc Ania i Bolek dysponują tym
samym kluczem $K = K_A = K_B$.

Ew. włamywacz zna A (oraz B) ale nie zna b (ani a) — nie wie, do jakiej potęgi
podnieść A (ew. B), żeby otrzymać klucz. Musiałby znaleźć
„dyskretny logarytm $a = \log_g(A)$ ”

Szyfrowanie asymetryczne — Diffie-Hellman

Metoda stosowana do zdalnego
ustalania klucza
szyfrowania symetrycznego
przez niepewny kanał

Ania	jawne	Bolek
	$n \in \mathbb{N}_{\geq 2}$ $g \in \mathbb{Z}_n$	
duża $a \in \mathbb{N}$ $A = g^a \bmod n$		duża $b \in \mathbb{N}$ $B = g^b \bmod n$
$K_A = B^a \bmod n$		$K_B = A^b \bmod n$

Diagram illustrating the exchange of values A and B between Ania and Bolek. A red arrow points from A in Ania's row to A in Bolek's row. A green arrow points from B in Bolek's row to B in Ania's row.



Whitfield
Diffie



Martin
Hellman

Ponieważ

$$\begin{aligned}
 K_A &\equiv_n B^a \equiv_n (g^b)^a = g^{ba} \\
 &= g^{ab} = (g^a)^b \equiv_n A^b \\
 &\equiv_n K_B
 \end{aligned}$$

więc Ania i Bolek dysponują tym
samym kluczem $K = K_A = K_B$.

Ew. włamywacz zna A (oraz B) ale nie zna b (ani a) — nie wie, do jakiej potęgi podnieść A (ew. B), żeby otrzymać klucz. Musiałby znaleźć „dyskretny logarytm $a = \log_g(A)$ ” — a to jest trudno wykonalne.

Szyfrowanie asymetryczne — podsumowanie

Szyfrowanie asymetryczne — podsumowanie

||

RSA

|

Diffie-Hellman

Szyfrowanie asymetryczne — podsumowanie

	RSA	Diffie-Hellman
służy do		

Szyfrowanie asymetryczne — podsumowanie

	RSA	Diffie-Hellman
służy do	bezpośredniego przesyłania wiadomości	

Szyfrowanie asymetryczne — podsumowanie

	RSA	Diffie-Hellman
służy do	bezpośredniego przesyłania wiadomości	ustalania klucza dla szyfru symetrycznego

Szyfrowanie asymetryczne — podsumowanie

	RSA	Diffie-Hellman
służy do	bezpośredniego przesyłania wiadomości	ustalania klucza dla szyfru symetrycznego
bezpieczeństwo opiera się na		

Szyfrowanie asymetryczne — podsumowanie

	RSA	Diffie-Hellman
służy do	bezpośredniego przesyłania wiadomości	ustalania klucza dla szyfru symetrycznego
bezpieczeństwo opiera się na	trudności rozkładu dużej liczby na czynniki	

Szyfrowanie asymetryczne — podsumowanie

	RSA	Diffie-Hellman
służy do	bezpośredniego przesyłania wiadomości	ustalania klucza dla szyfru symetrycznego
bezpieczeństwo opiera się na	trudności rozkładu dużej liczby na czynniki	trudności wyliczenia logarytmu dyskretnego dużej liczby