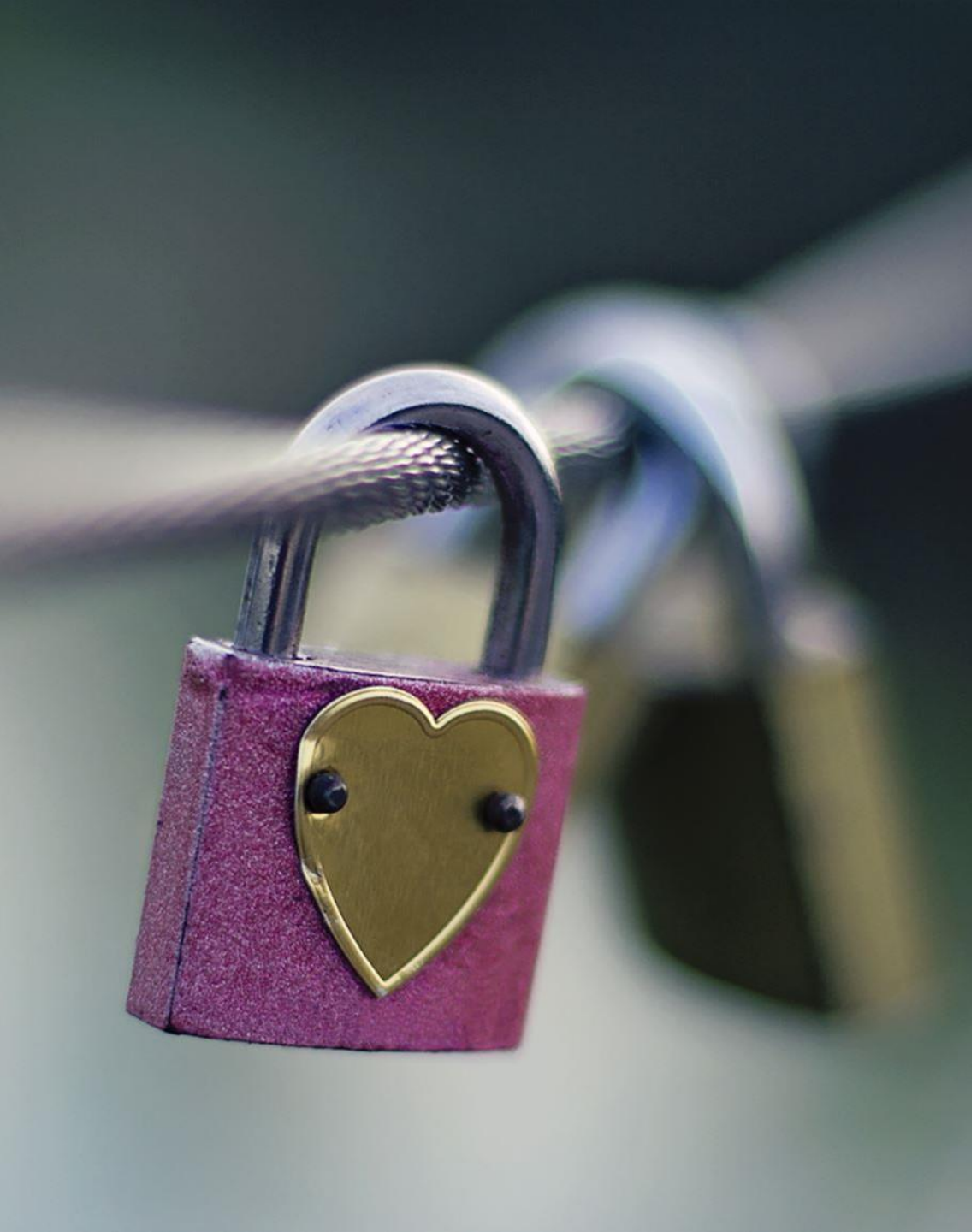
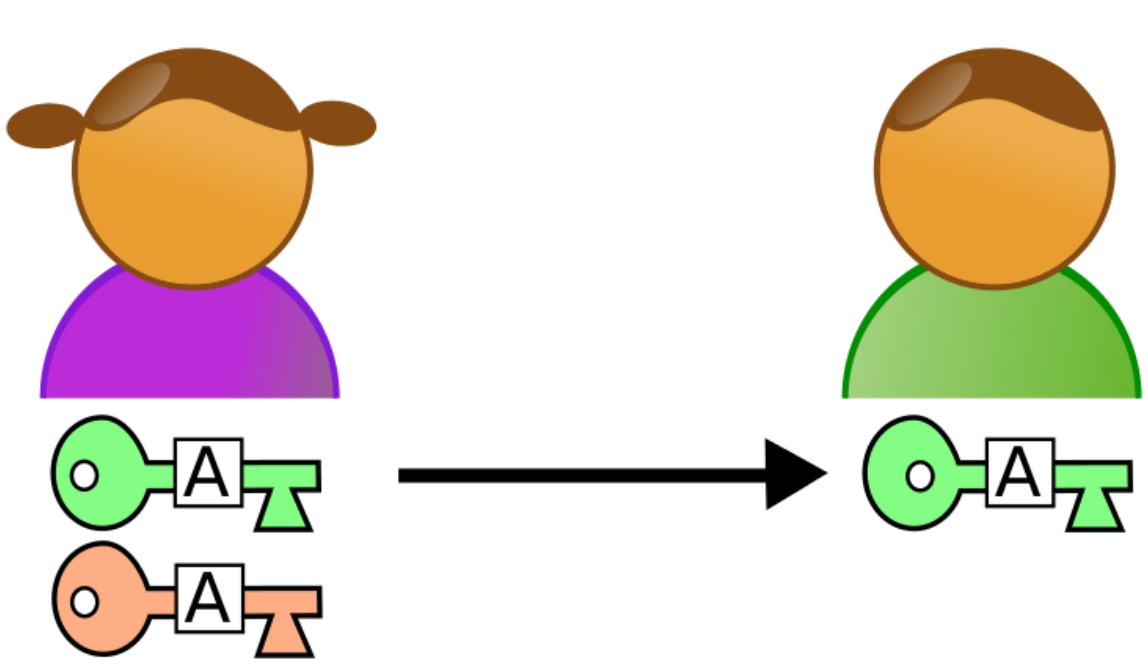
Szyfrowanie asymetryczne

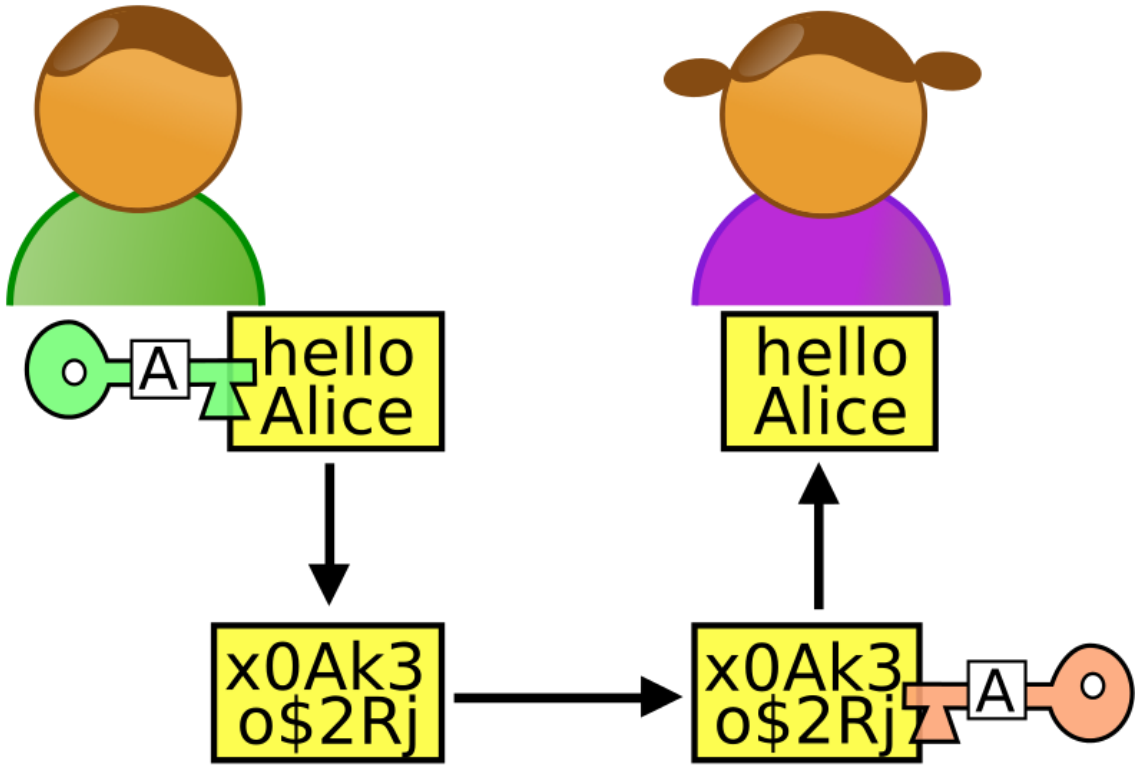
Damian Kurpiewski



Opis

- Kryptografia klucza publicznego
- Używane są dwa (lub więcej), powiązane ze sobą klucze
- Klucz prywatny i publiczny
- Klucz publiczny może być udostępniany bez utraty bezpieczeństwa danych
- Algorytmy: RSA, ElGamal, DSA, ECC…
- Wykorzystywane także w podpisach cyfrowych





Działanie

RSA

- Algorytm Rivesta-Shamira-Adlemana
- Zaprojektowany w 1977r.
- Jeden z najpopularniejszych asymetrycznych algorytmów kryptograficznych

RSA: generowanie kluczy

1. Wybieramy losowo dwie duże liczby pierwsze $\boldsymbol{p}$ i $\boldsymbol{q}$
2. Obliczamy $\boldsymbol{n = pq}$
3. Obliczamy wartość funkcji Eulera dla n: $\boldsymbol{\varphi(n) = (p-1)(q-1)}$
4. Wybieramy liczbę $\boldsymbol{e}$ $\boldsymbol{(1 < e < \varphi(n))}$ **względnie pierwszą z** $\boldsymbol{\varphi(n)}$
5. Znajdujemy liczbę d: $\boldsymbol{d \equiv e^{-1}(mod\ \varphi(n)))}$

- **Klucz publiczny** definiowany jest jako para liczb $\boldsymbol{(n, e)}$
- **Klucz prywatny** definiowany jest jako para liczb $\boldsymbol{(n, d)}$

RSA: Szyfrowanie i deszyfrowanie

- Dzielimy wiadomość na bloki m o wartości nie większej niż n
- Każdy z bloków szyfrujemy kluczem (n, e):

$$\boldsymbol{c \equiv m^e (mod\ n)}$$

- Zaszyfrowana wiadomość składa się z kolejnych bloków c
- Deszyfrowanie kluczem (n, d):

$$\boldsymbol{m \equiv c^d (mod\ n)}$$

Własności szyfrowania

C_{K_1}, C_{K_2} - szyfrowanie kluczami K_1 i K_2

D_{K_1}, D_{K_2} - deszyfrowanie kluczami K_1 i K_2

$$C_{K_1}\left(C_{K_2}(M)\right) = C_{K_2}\left(C_{K_1}(M)\right)$$

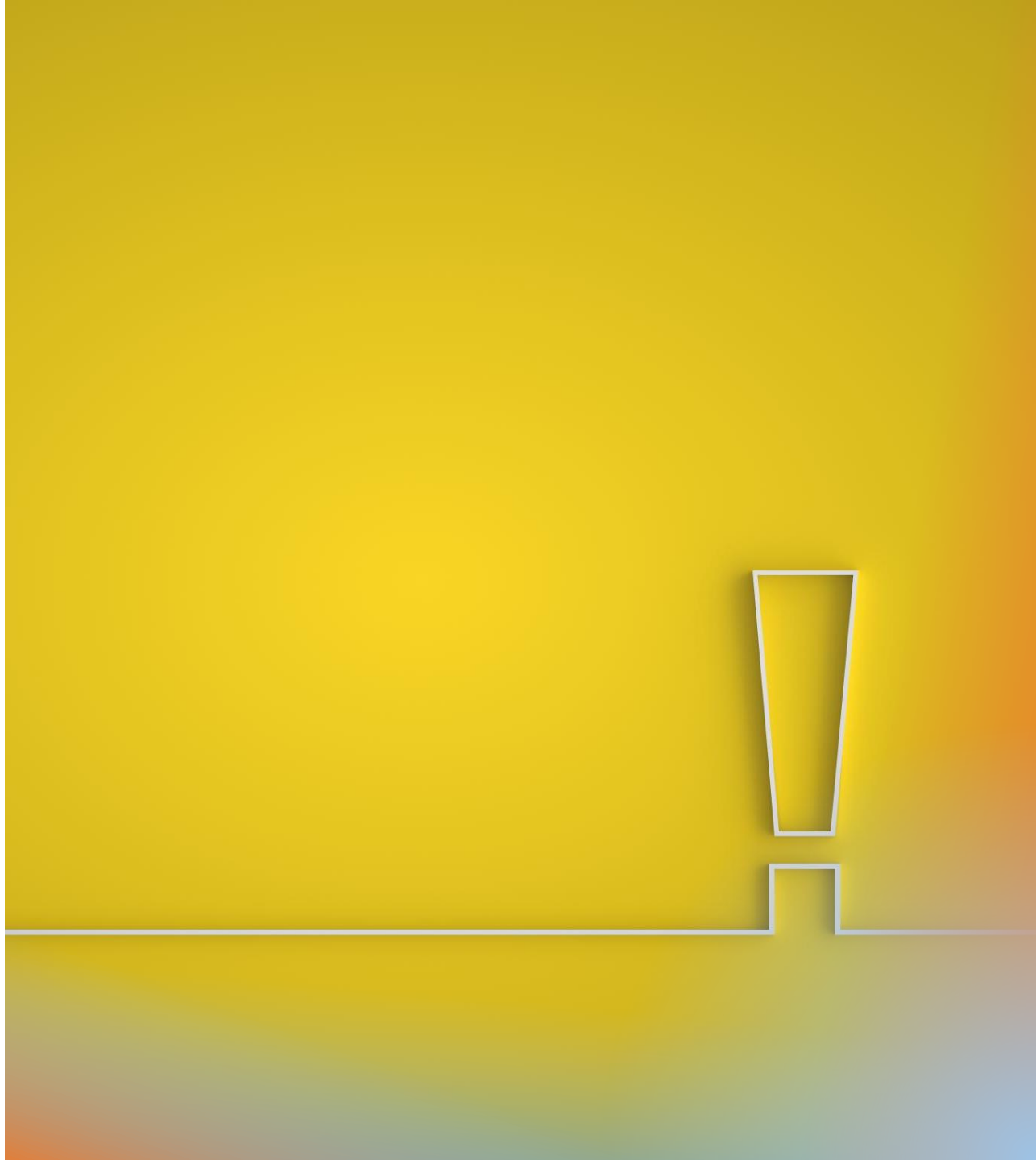
przemienność szyfrowania

$$D_{K_1}\left(D_{K_2}(M)\right) = D_{K_2}\left(D_{K_1}(M)\right)$$

przemienność deszyfrowania

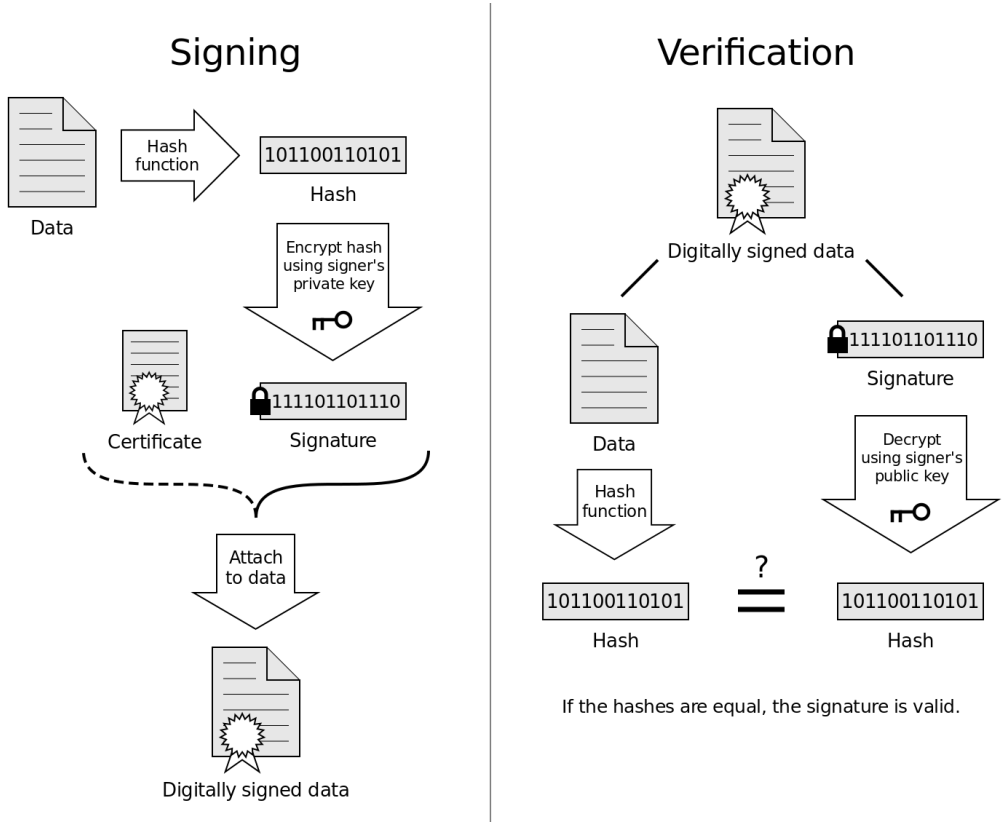
Podpis cyfrowy

- Sposób sprawdzenia autentyczności dokumentów i wiadomości elektronicznych
- Potwierdza nadawcę wiadomości
- Zapewnia, że wiadomość nie została zmieniona



Podpis cyfrowy: działanie

1. Tworzymy **skrót** wiadomości (używając funkcji haszującej)
2. Szyfrujemy go **kluczem prywatnym**
3. Wysyłamy razem z oryginalną wiadomością
4. Odbiorca potwierdza naszą tożsamość **odszyfrowując naszym kluczem publicznym**
5. Potwierdza, że wiadomość nie została zmieniona, **ponownie obliczając skrót wiadomości**



Podpis cyfrowy - działanie

Źródła

https://pl.wikipedia.org/wiki/Plik:Asymmetric_cryptography_-_step_1.svg

https://pl.wikipedia.org/wiki/Plik:Asymmetric_cryptography_-_step_2.svg

https://pl.wikipedia.org/wiki/RSA_(kryptografia)

https://pl.wikipedia.org/wiki/Kryptografia_klucza_publicznego

https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg