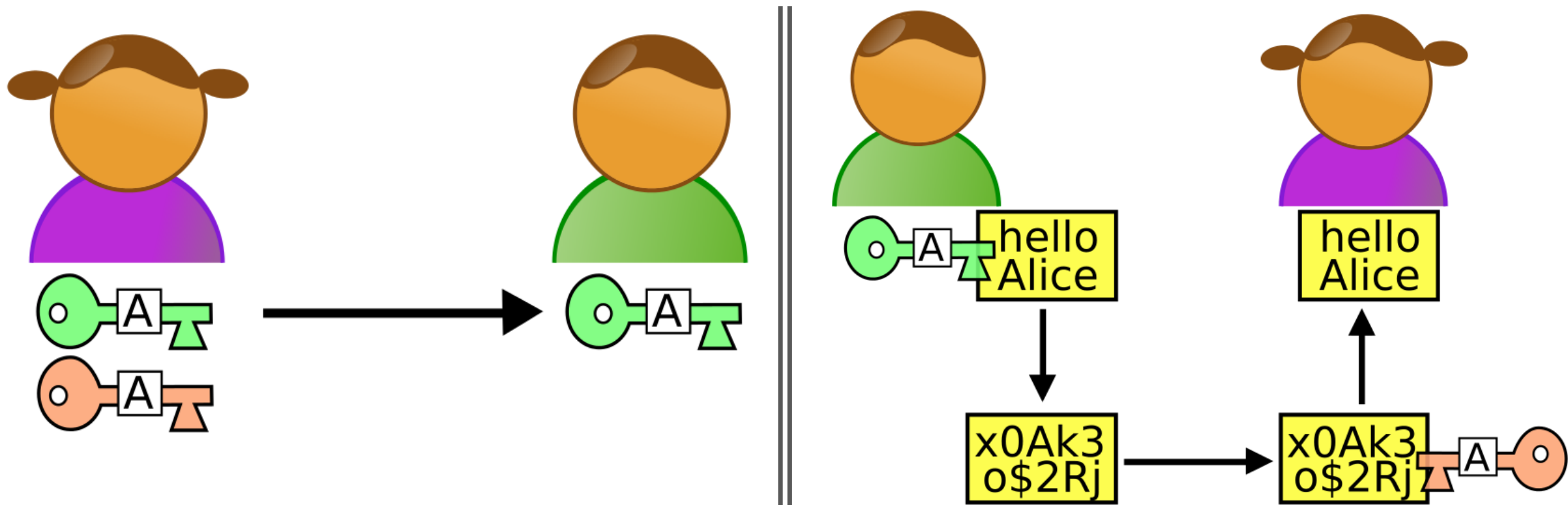


Szyfrowanie asymetryczne

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

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

- **Klucz publiczny** definiowany jest jako para liczb (n, e)
- **Klucz prywatny** definiowany jest jako para liczb (n, d)

RSA: Szyfrowanie i deszyfrowanie

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

$$c \equiv m^e \pmod{n}$$

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

$$m \equiv c^d \pmod{n}$$

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
- $C_{K_1} (C_{K_2} (M)) = C_{K_2} (C_{K_1} (M))$ - przemienność szyfrowania
- $D_{K_1} (D_{K_2} (M)) = D_{K_2} (D_{K_1} (M))$ - przemienność deszyfrowania

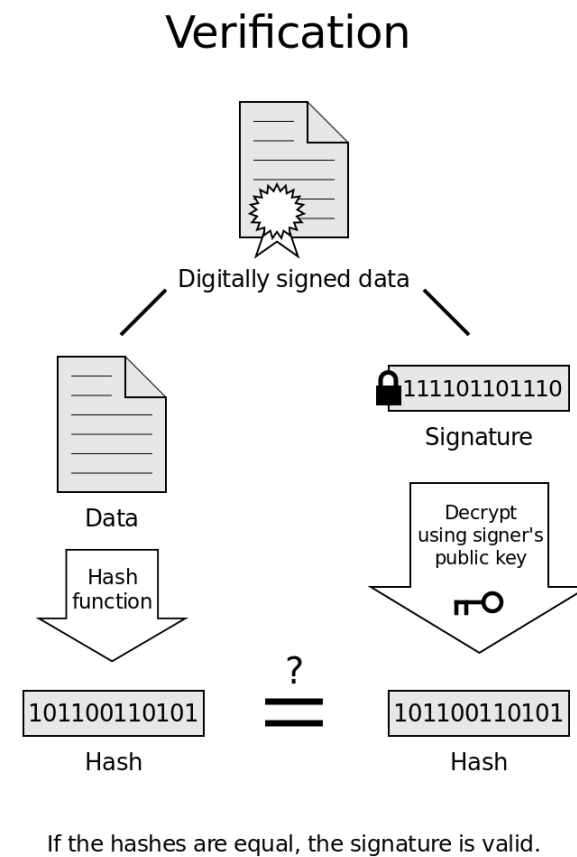
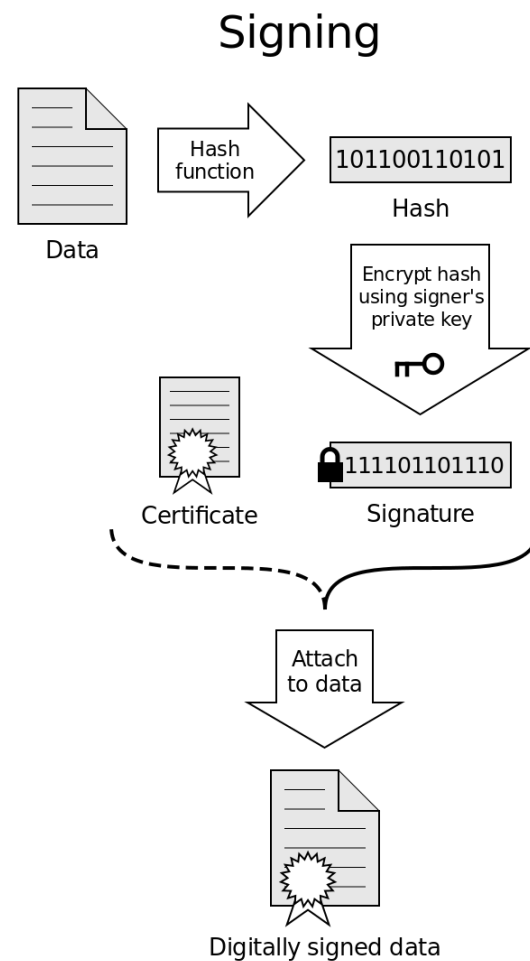
Podpis cyfrowy

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

Podpis cyfrowy - działanie

- Tworzymy **skrót** wiadomości (używając funkcji haszującej)
- Szyfrujemy go **kluczem prywatnym**
- Wysyłamy razem z oryginalną wiadomością
- Odbiorca potwierdza naszą tożsamość **odszyfrowując naszym kluczem publicznym**
- 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_1.svg)
- [https://pl.wikipedia.org/wiki/Plik:Asymmetric_cryptography - step 2.svg](https://pl.wikipedia.org/wiki/Plik:Asymmetric_cryptography_-_step_2.svg)
- [https://pl.wikipedia.org/wiki/RSA \(kryptografia\)](https://pl.wikipedia.org/wiki/RSA_(kryptografia))
- [https://pl.wikipedia.org/wiki/Kryptografia klucza publicznego](https://pl.wikipedia.org/wiki/Kryptografia_klucza_publicznego)
- [https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital Signature diagram.svg](https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg)