Kryptografia na potrzeby internetu

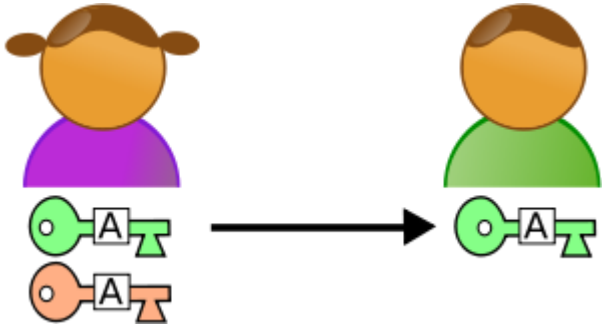
Własności internetu

- Komunikat wysłany e-mailem lub przeglądarką z jednego miejsca przechodzi przez wiele punktów pośrednich i może być łatwo:
  - Podejrzany – odczytany
  - Zmieniony bez śladu, że ktoś trzeci tego dokonał
  - Wygenerowany przez trzecią osobę bez śladu
- By stworzyć kanały zawierajace poufność i wiarygodność należy wprowadzić możliwość:
  - Szyfrowania
  - Podpisywania i weryfikacji podpisu

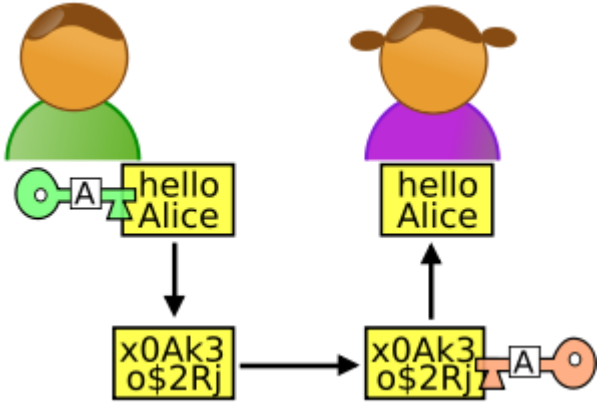
Kryptografia asymetryczna

- Jak przesłać hasło do szyfrowania lub wzorzec podpisu?
- Służy do tego kryptografia asymetryczna i hybrydowa

Najprostsza poufna korespondencja



- Alice przesyła Bobowi swój klucz publiczny



- Bob szyfruje kluczem publicznym wiadomość dla Alice
- Alice odszyfrowuje wiadomość swoim kluczem prywatnym

Przykład pary kluczy

- Klucz prywatny – duża liczba pierwsza
- Klucz publiczny – iloczyn klucza prywatnego i podobnie dużej liczby pierwszej

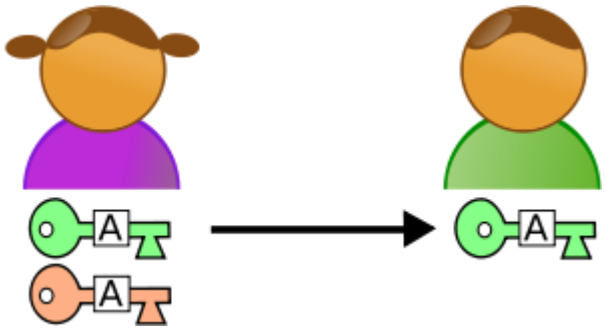
Odgadywanie klucza prywatnego na podstawie publicznego

```
For p:=2 to sqrt(x) do
  if x mod p = 0 then exit;
Write „Klucz prywatny to”
  p;
```

Złożoność obliczeniowa

- Wielkość wejścia $n = \log x$
- Liczba kroków algorytmu $x = 10^n$
- Złożoność obliczeniowa $O(10^n)$
- Problem NP-trudny obliczeniowo

Najprostsza podpisywanie korespondencji



- Alice przesyła Bobowi swój klucz publiczny

- Alice podpisuje kluczem prywatnym wiadomość dla Boba
- Bob sprawdza czy wiadomość pochodzi od Alice kluczem publicznym

Kryptografia hybrydowa(hptts://)

- Kryptografia asymetryczna jest znacznie bardziej czasochłonna niż kryptografia symetryczna i dlatego:
- Asymetrycznej komunikacji używa się by przesłać klucz szyfrowania symetrycznego
- Dalsza komunikacja odbywa się szyfrowaniem symetrycznym