Bezpieczeństwo w sieci I

a raczej: zabezpieczenia

wiarygodnosć, uwierzytelnianie itp.

Kontrola dostępu

Sprawdzanie tożsamości

Zabezpieczenie danych przed podsłuchem

Zabezpieczenie danych przed kradzieżą

Zabezpieczenie danych i systemów przed zmianą

Czy użytkownik (program) ma dostęp?

Czy użytkownik (program) jest tym,
za którego się podaje?

Jak bezpiecznie przesłać dane?

Jak chronić dane i systemy przed włamaniem?

Zaufanie

w wielu przypadkach *ufamy*,

że ktoś jest tym, za kogo się podaje

że zachowa się tak, jak chcemy

Zaufanie

w wielu przypadkach *ufamy*,

że e-mail jest od tej osoby, której adres jest w nagłówku

że inny użytkownik komputera, nie wykasuje nam plików

Zaufanie

Najczęszcze formy włamań wynika z błędnego zaufania: n.p. brak hasła lub łatwe hasło

Zaufanie

Najczęszcze formy włamań wynika z błędnego zaufania: n.p. brak hasła lub łatwe hasło

Inżyneria społeczna / social engineering

Inżyneria społeczna: wykorzystywanie zaufania

Wyłudzanie haseł czy innych poufnych danych

Oszustwa typu '419'

'Phishing'

Konie trojańskie

Zaufanie

w zabezpieczeniach (nie tylko w informatyce)
dążymy do eliminacji *potrzeby zaufania*

Identification / Identyfikacja

Authentication / Uwierzytelnianie

Authorisation / Autoryzacja

Identification / Identyfikacja

Authentication / Uwierzytelnianie

Authorisation / Autoryzacja

Identyfikacja

Deklaracja tożsamości

np. login

Identyfikacja

Deklaracja tożsamości

np. login

nie jest wiarygodna

Uwierzytelnianie

Sprawdzanie podanej tożsamości

Uwierzytelnianie

Tym, kim jesteś: dane biometryczne, DNA, podpis, głos

Tym, co masz: klucz, karta chipowa, dokument tożsamości

Tym, co wiesz: hasło, PIN

Uwierzytelnianie

dane biometryczne: wydają się pewne,
ale można je obejść / podrobić –
a nie można ich potem zmienić

fizyczne klucze / dokumenty: można podrobić
albo ukraść → *klucze jednorazowe, tokeny*

pamięć: najpewniejsze, ale najtrudniejsze

Autoryzacja

Sprawdzanie czy *uwierzytelniona* tożsamość ma prawo wykonać daną operacje.

Czasem równoczesna / równoważna z uwierzytelnianiem
– n.p. access kontrol / kontrola dostępu

Przykłady kontroli dostępu

Wjazd do kraju z paszportem

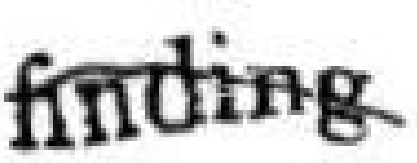
Karty magnetyczne do drzwi

Logowanie się z hasłem

CAPTCHA

CAPTCHA

do odróżnienia *człowieka* od *komputera*



Szyfrowanie

Zabezpiecza dane przed osobami (programami) które nie mają do nich praw albo nie powinny je przeczytać

Szyfrowanie

Zabezpiecza dane przed osobami (programami) które nie mają do nich praw albo nie powinny je przeczytać

Pozwala też chronić dane przed zmianą przez nieuprawione osoby (programy)

Szyfrowanie

Do szyfrowania potrzebny jest *klucz*

Szyfrowanie

Do szyfrowania potrzebny jest *klucz*

Jak przesłać klucz do odbiorcy, bez ujawniania go innym?

Szyfrowanie

Do szyfrowania potrzebny jest *klucz*

Jak przesłać klucz do odbiorcy, bez ujawniania go innym?

Kryptografia asymetryczna

Kryptografia asymetryczna

Dwa klucze:

klucz publiczny

klucz prywatny

Kryptografia asymetryczna

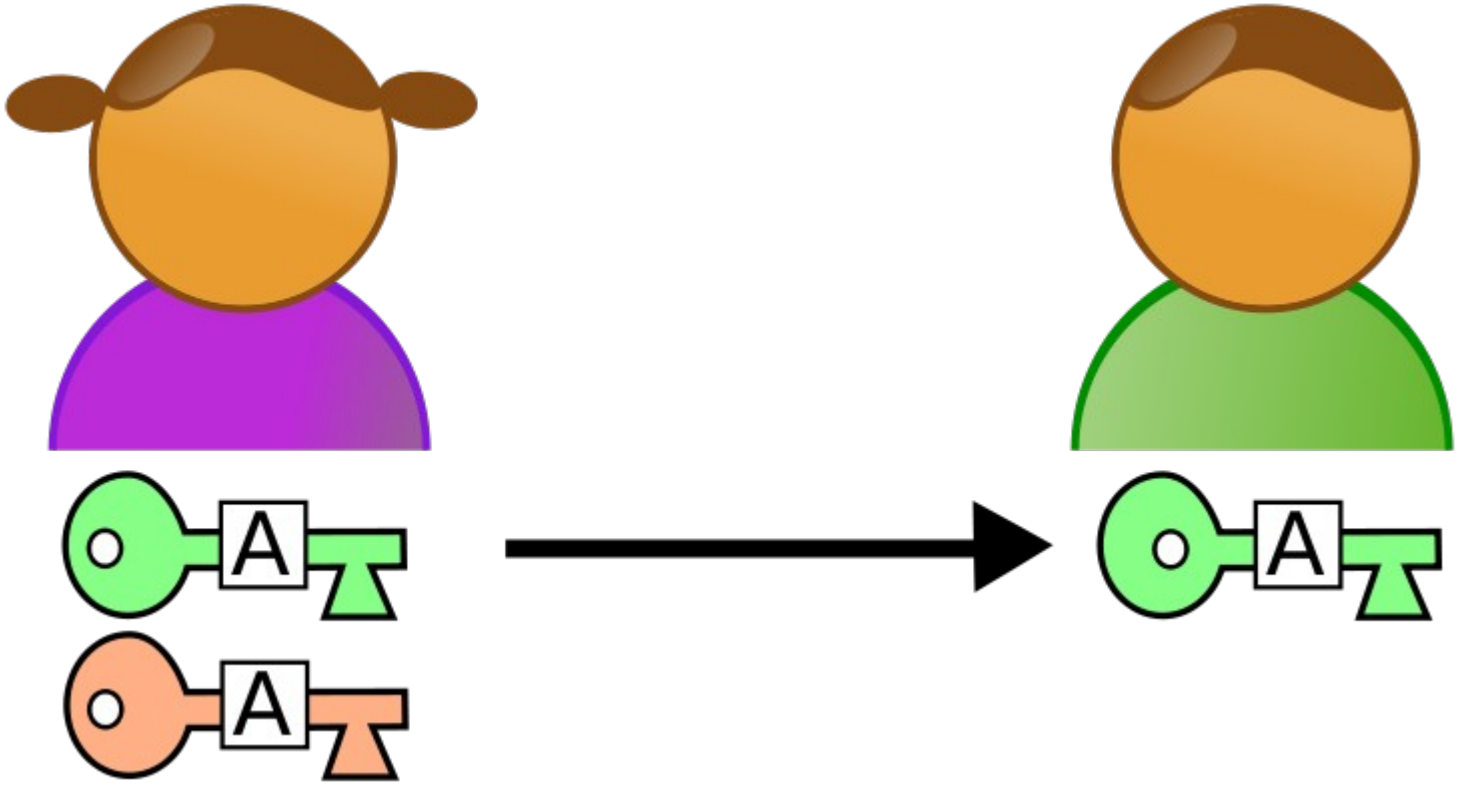
Oficjalnie wynaleziona przez Hellman, Diffie oraz niezależnie Merkle w 1976

Kryptografia asymetryczna

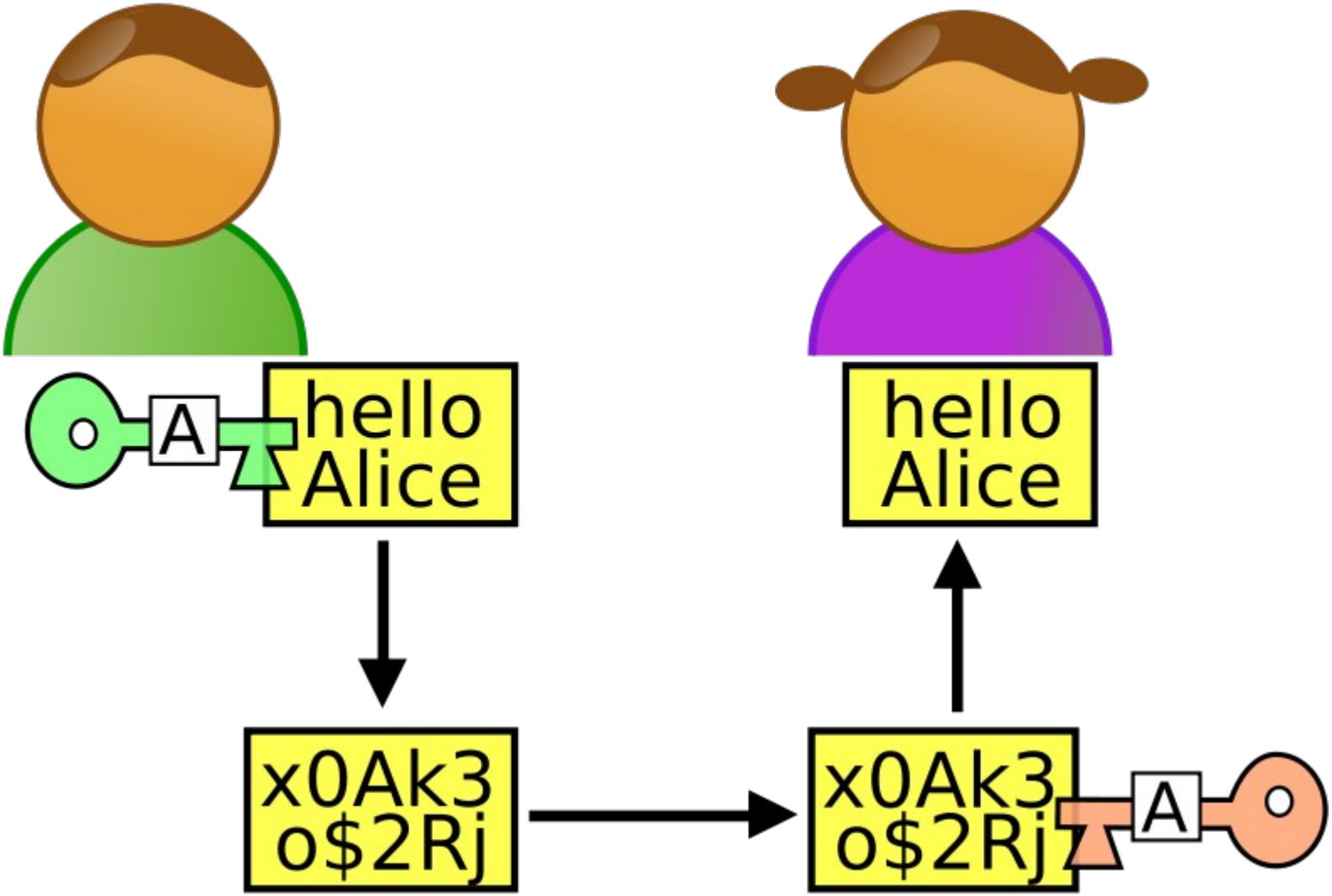
Oficjalnie wynaleziona przez Hellman, Diffie oraz niezależnie Merkle w 1976

Obecnie wiemy, że przez Ellisa w GHCQ już w 1965

Kryptografia asymetryczna



Kryptografia asymetryczna



Kryptografia asymetryczna

Kluczem publicznym można jedynie *zaszyfrować* wiadomość, a *nie* odszyfrować

Kryptografia asymetryczna

Kluczem publicznym można jedynie *zaszyfrować* wiadomość, a *nie* odszyfrować

Klucz publiczny można bezpiecznie przesłać

Kryptografia asymetryczna

Operacje jednokierunkowe

Kryptografia asymetryczna

Operacje jednokierunkowe

czyli operacja (funkcja) w jedną strone jest łatwa, a odwrócenie jej (odwrotność funkcji) jest trudna do wykonania

Kryptografia asymetryczna

Operacje jednokierunkowe

RSA mnożenie (łatwe) / faktoryzacja (trudne)

DSA potęgowanie moduło (łatwe)
/ zalezienie logarytmu dyskretnego (trudne)

Kryptografia asymetryczna

Operacje jednokierunkowe

Zawsze musi być funkcja odwrotna – inaczej nie można by odszyfrować

Kryptografia asymetryczna

Operacje jednokierunkowe

Projektujemy system tak, że wykonanie funkcji odwrotnej bez klucza (czyli łamanie szyfru) jest bardzo czaslochłonne

błędy w algorytmie

błędy w implementacji (n.p. nielosowy generator liczb (pseudo-)losowych

wzrost mocy obliczeniowej
(w zasadzie *zgadywanie*)

Słowniki haseł

liczba możliwych haseł 8-znakowych korzystając jednynie z liter alfabetu angielskiego, bez cyfr czy dużych liter to 26^8 =

208 827 064 576

Słowniki haseł

liczba słow w zwykłym słowniku to zaledwie rzędu

100 000

Systemy hybrydowe

Używa kryptografie symetryczną (jeden klucz)
i kryptografię asymetryczną

Systemy hybrydowe

Najpierw klucz systemu symetrycznego jest przesłany w postaci zaszyfrowanej systemem asymetrycznym

Pozostałe wiadomości są szyfrowane tym kluczem

Systemy hybrydowe

Szybkie $\longrightarrow$ stosowane w komunikacji 'na żywo'
gdzie ważna jest prędkość szyfrowania i gdzie
nie znana jest całkowita ilość danych do przesłania

SSH

SSL/TLS

Szyfrowane telefony

Podpis cyfrowy

do uwierzytelniania widomości

Podpis cyfrowy

do uwierzytelniania widomości

czy ta wiadomość rzeczywiscie pochodzi od tego nadawcy?

kryptografia asymetryczna

Podpis cyfrowy - nadawca

piszemy wiadomość

szyfrujemy skrót wiadomości (*hash)* kluczem prywatnym

dołączamy tak zaszyfrowany skrót do wiadomości

Podpis cyfrowy - odbiorca

posiada (niezależnie) klucz publiczny nadawcy

odszyfrowywuje zaszyfrowany skrót

liczy własny skrót

porównuje oba skróty

Podpis cyfrowy

W niektorych systemach (n.p. RSA) klucze prywatne i publiczne są symetryczne: oba mogą szyfrować i odszyfrowywać

→ klucze używane do szyfrowania i do podpisów są te same

Podpis cyfrowy

W innych systemach (n.p. ElGamal) klucze prywatne i publiczne są asymetryczne: tylko jeden szyfruje a drugi odszyfrowywuje

→ klucze używane do szyfrowania i do podpisów są różne

Podpis cyfrowy

Niektóre systemy służą tylko do podpisów (n.p. DSA)

Podpisy cyfrowe i szyfrowanie asymetryczne

pozostaje problem wiarygodności kluczy publicznych

Podpisy cyfrowe i szyfrowanie asymetryczne

pozostaje problem wiarygodności kluczy publicznych

Infrastruktura Kluczy Publicznych
(Public Key Infrastructure / PKI)

sieć zaufania / web of trust

Infrastruktura Kluczy Publicznych

CA certificate authority / urząd certyfikacji

RA registration authority / urząd rejestracji

Certyfikaty

dane podpisane cyfrowo przez stronę, której ufamy

- klucz publiczny właściciela certyfikatu
- imię i nazwisko
- nazwa organizacji czy firmy
- czas w jakim certyfikat jest ważny
- sposób weryfikacji certyfikatu