Podstawy kryptografii

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2023/2024

inf.ug.edu.pl/~amb/

Kryptografia klucza prywatnego a kryptografia klucza publicznego

Zarządzanie kluczami prywatnymi

- „Sprzeczność" kryptografii klucza prywatnego:
  – kryptografia służy bezpiecznemu przekazaniu tekstu
  – ale jak bezpiecznie przekazać klucz prywatny?
- Dwa powody
  – klucze mogą być/są krótsze niż teksty jawne
  – odległość w czasie pomiędzy wymianą a użyciem klucza
- Wymiana klucza
  – koniecznie w bezpośrednim kontakcie zainteresowanych
  – dla n osób potrzeba $\frac{n(n-1)}{2}$ kluczy, po $n-1$ dla każdego
  – wymianę może organizować centrum
    - z każdym uczestnikiem j ma uzgodniony klucz K_j,
    - zainteresowanym użytkownikom przekazuje klucz sesyjny $E(K_\ell, K_{\ell j}))$, $E(K_j, K_{\ell j}))$
  – ale bezpieczeństwo całej organizacji zależy od bezpieczeństwa centrum

Rewolucja w kryptografii

- Diffie/Hellman (USA) 1976 – idea kryptografii asymetrycznej
  – są dwa różne klucze
  – klucze stanowią parę: $Dec(K_d, Enc(K_e, m)) = m$ dla wszystkich m
  – znajomość jednego klucza (publiczny) nie ujawnia drugiego (prywatny)
- Trzy zastosowania
  – szyfrowanie bez wstępnej wymiany klucza
  – podpis cyfrowy (niezaprzeczalność)
  – protokół uzgodnienia wspólnego klucza („wymiana")
- Diffie/Hellman
  – podali implementację protokołu wymiany klucza (wystarcza do nawiązania łączności i szyfrowania)
  – jedna z implementacji szyfrowania i podpisu oparta jest na ich ideach

Kryptografia asymetryczna, szyfrowanie i podpis cyfrowy

- Dwa różne klucze: publiczny – K_e oraz prywatny – K_d
  – Alicja szyfruje wiadomość do Bolka: $m \mapsto E(K_e, m) = c$, być może niedeterministycznie, używa jego klucza publicznego
  – Bolek odszyfrowuje szyfrogram: $c \mapsto D(K_d, c) = m$
  – tylko Bolek zna klucz prywatny K_d, nawet Alicja nie może odszyfrować tej wiadomości
  – klucz publiczny Bolka może być szeroko rozpowszechniony („książka telefoniczna")
- Podpis cyfrowy: zamiana rolami kluczy, prywatny – K_e oraz publiczny – K_d
  – Alicja szyfruje wiadomość swoim kluczem prywatnym
  – Bolek/każdy może ją odszyfrować kluczem publicznym Alicji
  – co jest dowodem, że tylko Alicja mogła to wykonać
  – założenie: wiemy, że klucz prywatny zna tylko Alicja

Atak *man in the middle* (pośrednik)

- – Mariola jako Alicja → Bolek: podaje klucz publiczny
  – Bolek → Mariola jako Alicja: szyfruje wiadomość dla Alicji
  – Mariola jako Bolek → Alicja: podaje klucz publiczny
  – Alicja → Mariola jako Bolek: szyfruje wiadomość dla Bolka
  – Alicja i Bolek myślą, że rozmawiają ze sobą
  – ale cała korespondencja przechodzi przez Mariolę
- Jeden z najtrudniejszych ataków do odparcia
  – konieczność uwierzytelniania uczestników
  – musimy wiedzieć, że klucz publiczny Alicji jest rzeczywiście kluczem publicznym Alicji

Kryptografia asymetryczna, podpis

- W kryptografii symetrycznej uwierzytelnianie jest łatwe
  – Bolek wie, że skoro wiadomość jest zaszyfrowana wspólnym kluczem K_{AB}, to autorem musi być Alicja
  – ale nie może tego udowodnić przed sądem, skoro on też może przygotować taką wiadomość
- W kryptografii asymetrycznej tylko Alicja może zaszyfrować wiadomość swoim kluczem prywatnym
  – nie tylko Bolek może to sprawdzić, każdy może
  – w zasadzie sprawdzić można jedynie, że K_e oraz K_d stanowią parę
  – pozostaje problem związku Alicji z tą parą kluczy
- Mariola ogłasza, że klucz publiczny należy do Alicji
  – i podpisuje dokument
  – Bolek weryfikuje, że podpis został złożony przez pasujący klucz prywatny
  – ale czy podpis został złożony przez Alicję?

Kryptografia asymetryczna, cechy

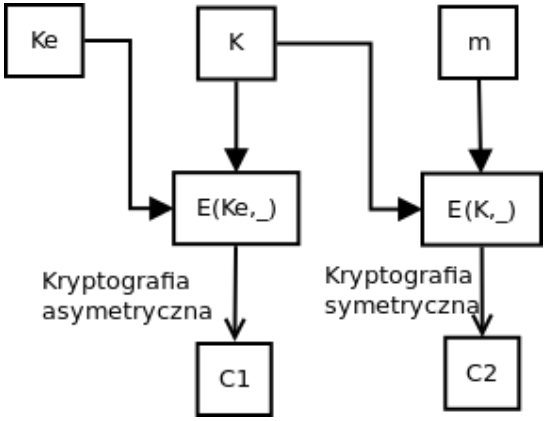
- Zalety:
  – nie ma konieczności wcześniejszej wymiany tajnego klucza
  – klucz prywatny nie jest z nikim wymieniany
  – jest tylko jeden taki klucz
- Wady:
  – zdecydowanie mniejsza wydajność
    - więcej się szyfruje i uwierzytelnia (serwery)
    - zasoby są mniejsze (karta kryptograficzna) niż w kryptografii symetrycznej
  – problem uwierzytelnienia klucza publicznego
    - Mariola ogłasza, że klucz publiczny należy do Alicji
    - a Bolek sądzi, że komunikuje się z Alicją
    - oraz, że ona jest autorką podpisanych dokumentów

Teoretyczne własności kryptografii asymetrycznej

- Tw.: odporność na atak ze znanym kryptogramem jest równoważna odporności na atak z wybranym tekstem jawnym
  – dw.: ten drugi atak zakłada dostęp do wyroczni szyfrującej na życzenie
  – ale klucz publiczny jest jawny i każdy może szyfrować
- Wniosek: szyfr odporny na atak musi być niedeterministyczny
- Tw.: odporność na atak przy wielokrotnym szyfrowaniu jest tak sama (bez dowodu)
- Tw.: nie istnieje doskonale bezpieczny szyfr kryptografii asymetrycznej
  – dw.: dla każdego potencjalnego klucza prywatnego sprawdzamy, czy jest odwrotny do znanego klucza publicznego
  – jeśli złożoność nie jest barierą, to klucz zostanie znaleziony

Szyfr hybrydowy

- Szyfrowanie
  – wygenerowanie klucza symetrycznego K
  – przesłanie K za pomocą kryptografii asymetrycznej: $C_1 = Enc(K_e, K)$
  – użycie K w kryptografii symetrycznej: $C_2 = Enc(K, m)$
- Odszyfrowanie
  – najpierw klucz sesyjny z C_1: $K = Dec(d, C_1)$
  – potem wiadomość z C_2: $m = Dec(K, C_2)$



Zalety szyfru hybrydowego

- Wydajność jak dla kryptografii symetrycznej (plus niewielki narzut na klucz sesyjny)
- W sumie jest to kryptografia klucza publicznego
  – nie ma potrzeby wymiany klucza prywatnego
- Tw.: jeśli oba szyfry są odporne na atak ze znanym kryptogramem, to szyfr hybrydowy jest odporny na atak z wybranym tekstem jawnym
  – cześć asymetryczna ma tę własność automatycznie
  – klucz sesyjny jest wybierany losowo i jednorazowo, więc część symetryczna też ma tę własność
- A więc szyfr strumieniowy może być spokojnie używany jako część szyfru

Podpis cyfrowy w praktyce

- Podpis cyfrowy:
  – Bolek szyfruje wiadomość swoim kluczem prywatnym
  – ale wydajność nie pozwala na szyfrowanie dłuższych wiadomości
- Rozwiązanie:
  – Bolek oblicza skrót wiadomości $h(m)$, szyfruje go kluczem prywatnym $S(h(m))$, przekazuje parę $\langle m, S(h(m))\rangle$
  – każdy może zweryfikować podpis kluczem publicznym, tzn. sprawdzić, że $h(m) = V(S(h(m)))$
  – de facto weryfikuje podpis jedynie skrótu wiadomości
- Cechy podpisu skrótu
  – musimy wierzyć, że znajomość $h(m)$ oznacza znajomość m
  – można składać podpis pod nieznanym dokumentem

Konsekwencje ataku na funkcję skrótu

- Atak Alicji:
  – Alicja ma dwie wersje wiadomości m_1 oraz m_2, jedna korzystna dla niej, drugą skłonny jest podpisać Bolek
  – Alicja modyfikuje każdą z wiadomości, otrzymuje dwa zestawy: m_1 oraz m_2, oblicza skróty i szuka wspólnego
  – Bolek podpisuje m_2, tzn. szyfruje $S(h(m_2))$
  – Alicja twierdzi, że Bolek podpisał m_1,
  – dowodzi, że $h(m_1) = V(S(h(m_2)))$, ponieważ $h(m_1) = h(m_2)$

Obrona przed atakiem na funkcje skrótu

- Długość funkcji skrótu: dwa razy dłuższa niż długość klucza/bloku w kryptografii symetrycznej, od 128 bitów, raczej 160, 224 i więcej
- Obliczanie skrótu wiadomości razem z informacją o jej długości
  – trudno znaleźć m oraz m' o identycznej wartości skrótu, jeszcze trudniej, jeśli muszą mieć tę samą długość
- Modyfikacja podpisywanej wiadomości
  – jeśli Alicja podsuwa Bolkowi przygotowaną wiadomość m_2 do podpisu, Bolek odmawia podpisania, godzi się dopiero po dokonaniu nieistotnej zmiany