

Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2023/2024

inf.ug.edu.pl/~amb/

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 klucza prywatnego a kryptografia klucza publicznego

Kryptografia asymetryczna, szyfrowanie i uwierzytelnianie

- Dwa różne klucze: publiczny – K_e oraz prywatny – K_d
 - Alicja szyfruje wiadomość do Boleka: $m \mapsto E(K_e, m) = c$, 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 Boleka 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
 - Mariola jako Bolek → Alicja: podaje klucz publiczny
 - Alicja → Mariola jako Bolek: szyfruje wiadomość
 - Alicja i Bolek myślą, że rozmawiają ze sobą
 - ale cała korespondencja przechodzi przez Mariolę
- Jeden z najtrudniejszych ataków do odparcia
 - konieczność uwierzytelniania uczestników

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

Kryptografia asymetryczna, podpis

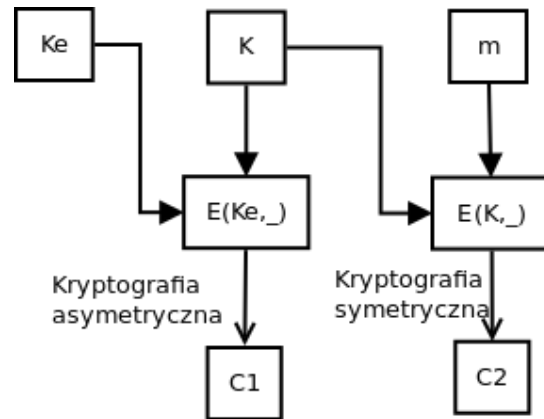
- W kryptografii symetrycznej uwierzytelnianie jest łatwe
 - Bolek wie, że skoro wiadomość jest zaszyfrowana wspólnym kluczem K_{AB} , to autorem musi być Alicja
 - ale nie może tego udowodnić przed sądem, on też może przygotować taką wiadomość
- W kryptografii asymetrycznej tylko Alicja może zaszyfrować 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

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 wyroczeni 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: $C_1 = Enc(e, K)$
 - 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 : $m = Dec(K, C_2)$

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

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
 - część 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

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 analogiczna długość w kryptografii symetrycznej, od 128 bitów
- 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 może odmówić podpisania, zgodzi się dopiero po dokonaniu nieistotnej zmiany