17.01.04

Kryptografia i bezpieczeństwo

WPPT 2003, informatyka inżynierska

Zadania przygotowawcze na kolokwium nr 2

1. Czy kryptogram C tekstu D uzyskany przy pomocy klucza prywatnego w algorytmie RSA może być uznany za podpis elektroniczny pod D?
2. W algorytmie podpisów ElGamala zamiast parametru losowego r zastosowano $H(D)$, gdzie D jest podpisywanym dokumentem. Dlaczego jest to rozwiązanie złe?
   Jak zaimplementować generowanie podpisów ElGamala, gdy nie dysponujemy żadnym wiarygodnym źródła losowości?
3. Chcielibyśmy dla podpisów RSA, podobnie jak w przypadku ElGamala, mieć możliwość składania podpisów kilkukrotnie pod tym samym dokumentem (aby to miało sens, uzyskiwane podpisy muszą być różne). Zaproponuj jakieś sensowne rozwiązanie.
4. Zaprojektować schemat działania karty mikroprocesorowej, która ma służyć jako ładowalna karta telefoniczna.
5. Ostatnio dużo się mówi w prasie o zjawisku czyszczenia kont klientów korzystając z danych uzyskanych przez czytniki kart i mikrokamery. Jaki jest mechanizm ataku? W jaki sposób uodpornić się przed tym atakiem przy pomocy kart mikroprocesorowych.
6. Czy w GSM komórka ma pewność, że połączyła się ze stacją bazową wlaściwej firmy (zakładamy, że połączenie z rozmówcą zostało nawiązane)?
7. Sprawdź, czy zwiększenie długości sumy kontrolnej generowanej przez Clipper załatwiłoby wszystkie problemy omawiane na wykładzie.
8. Zaproponuj jakiś wygodny i bezpieczny system generowania haseł jednorazowych.
9. Czy Kerberos jest odporny na atak man-in-the-middle? Uzasadnij.
10. Porównaj jak można unieważnić klucze w pgp i w klasycznej architekturze z Centrami Certyfikacji kluczy.
11. Przeczytaj manual do ssh (np. poprzez man ssh w systemach Unixowych). Porównaj metody uwierzytelniania wersji 1 i 2 protokołu.
12. Standardowy system haseł w UNIXie używa hashowania jako podstawy. Dlaczego hasła nie są przechowywane w postaci zaszyfrowanej tajnym kluczem?
13. Wykaż na przykładzie, że atak typu known plaintext może być skuteczny, gdy atak known ciphertext jest niemożliwy do przeprowadzenia. (Znasz ten przykład!)
14. Załóż, że w przypadku szyfrowania algorytmem RSA możesz ustawiać na karcie pojedynczy bit klucza na 1 (na trwałe). Czy możesz w ten sposób odczytać klucz z karty?
15. Policz, ile średnio zajęłoby czasu złamanie DES-a metodą brute-force, jeśli dysponowałbyś parą tekst jawny - kryptogram, oraz posiadałbyś układ składający się z 2^{10} jednostek, z których każdy potrafiłby wyliczyć 2^{10} kryptogramów na sekundę?