Kodowanie i bezpieczeństwo informacji

Lista nr 5 na 26 III - 6 IV 2012

Zadanie 1 Korzystając z Chińskiego Twierdzenia o Resztach pokaż, że jeżeli $N = pq$, $gcd(p, q) = 1$, oraz $ed = 1 \bmod \phi(N)$ to dla wszystkich $x \in Z_N^*$ zachodzi $(x^e)^d = x \bmod N$. Czy ta równość zachodzi też dla $x \in Z_N$?

Zadanie 2 Niech $N = pq$, gdzie p, q są różnymi liczbami pierwszymi. Pokaż, że jeżeli zna się zarówno $\phi(N)$ jak i N to można znaleźć p i q w wielomianowym czasie.

Zadanie 3 Alicja i Bob chcą uzgodnić klucz sesyjny za pomocą protokołu Diffie-Hellmana. Wyjaśnij w szczegółach jak przeprowadzić atak (*man-in-the-middle*) na protokół, tak aby po jego wykonaniu adwersarz miał uzgodniony z Alicją klucz k_A, oraz klucz k_B z Bobem.

Zaproponuj modyfikacje protokołu, które uniemożliwią taki atak.

Zadanie 4 Przeanalizuj następujący protokół uzgadniania klucza:

1. Alicja wybiera $k, r \leftarrow \{0,1\}^n$ losowo; wysyła $s := k \oplus r$ do Boba.
2. Bob wybiera $t \leftarrow \{0,1\}^n$ losowo i wysyła $u := s \oplus t$ do Alicji.
3. Alicja oblicza $w := u \oplus r$ i przesyła w do Boba.
4. Alicja do dalszej komunikacji używa k, Bob używa $w \oplus t$.

Pokaż, że Alicja i Bob korzystają z tego samego klucza. Przeanalizuj bezpieczeństwo tego protokołu (udowodnij jego bezpieczeństwo, bądź pokaż jak taki protokół zaatakować).

Zadanie 5 W pewnej firmie moduły kluczy RSA przacowników są takie same. Pokaż, że z kryptogramu tej samej wiadomości wysłanej do pracowników o kluczach publicznych $[N, e_1]$ oraz $[N, e_2]$ gdzie $e_1 \neq e_2$ można wydobyć wiadomość.

Innymi słowy pokaż, że znając: N, $c_1 = m^{e_1} \bmod N$ i $c_2 = m^{e_2} \bmod N$ można wyliczyć m. Jakie dodatkowe założenie trzeba przyjąć o e_1, e_2, aby móc wyliczyć m?

Zadanie 6 Sprawdź jakie dane przechowywane są jako klucz prywatny

```
openssl rsa -noout -text -in privkey.pem
```

Jakie N (modulus) i e (publicExponent) ma Twój klucz? Czy jeżeli posiadasz $e = 65537$ to powinnaś/powinieneś się niepokoić (vide: zadanie 5)?

Z jakich powodów pamiętane są p, q (prime1, prime2)? Pokaż jak można je wykorzystać, aby zwiększyć efektywność podpisywania/deszyfrowania. Jaki jest zysk wydajności - porównując do przypadku w którym zapomnianoby o p i q?