28 maja 2024

Zadania z kryptografii, lista nr 9

1. Jak można nie znając klucza tajnego RSA Alicji wyprodukować jakąś parę $(m, m^d \bmod n)$ czyli parę: wiadomość, podpis. W jaki sposób ogranicza to stosowalność podpisów RSA?

2. Załóżmy, że wybrano i, j takie, że $j \perp (p-1)$ oraz

$$r = g^i y^j \bmod p$$

$$s = -rj^{-1} \bmod p-1$$

$$m = -is \bmod p-1.$$

   Pokaż, że (r, s) jest podpisem ElGamala dla m. Jakie to ma konsekwencje dla bezpieczeństwa algorytmu podpisów ElGamala.

3. Załóżmy, że (r, s) jest podpisem ElGamala dla m. Niech h, i, j będą liczbami całkowitymi takimi, że $0 \leq h, i, j \leq p-2$ i $\gcd(hr - js, p-1) = 1$. Pokaż, że jeśli

$$r' = r^h g^i y^j \bmod p$$

$$s' = sr'(hr - js)^{-1} \bmod p-1$$

$$m' = r'(hm + is)(hr - js)^{-1} \bmod p-1,$$

   to (r', s') jest podpisem ElGamala dla m'.

4. Pokaż jakie niebezpieczeństwo niesie za sobą dwukrotne użycie tego samego losowego parametru r $(r = g^r)$ podpisu ElGamala. Powtórz to samo dla DSA.

5. W algorytmie podpisów ElGamala losowane jest k na podstawie którego obliczana jest pierwsza część podpisu $r = g^k \bmod p$. Załóżmy, że Alicja zamiast wylosować uczciwie k podstawi zamiast niego tajną wiadomość μ. Pokaż jak Bob będący w spisku i znający klucz tajny Alicji może z podpisu odzyskać wiadomość μ.

6. Rozważmy następującą wariację schematu podpisów ElGamala. Klucz tajny: $x (x \perp p-1)$. Klucz jawny: $p, g, y = g^x \bmod p$. Podpis pod tekstem m to para (r, s) tworzona następująco. Losujemy k i $r = g^k \bmod p$. Inaczej niż w oryginalnym schemacie ElGamala $s = (m - rk)x^{-1} \bmod (p-1)$.

   (a) Pokaż jak należy weryfikować podpis.

   (b) Jaką korzyść w złożoności uzyskujemy w porównaniu z oryginalnym schematem ElGamala?

7. Inny protokół rzutu monetą przez telefon:

   - Alicja wybiera $n = pq$ (p, q – pierwsze i przystające do 3 mod 4) i wysyła do Boba n.
   - Bob wybiera $x \in \mathbb{Z}_n$ i przesyła Alicji $y = x^2 \bmod n$.
   - Alicja oblicza z, takie że $z^2 \equiv y \bmod n$ i odsyła je do Boba.
   - Jeśli $x \not\equiv \pm z \bmod n$, to Bob faktoryzuje n.
   - Bob wygrywa, jeśli potrafi sfaktoryzować n.

   Dlaczego prawdopodobieństwo wygranej Boba wynosi 1/2? Wyjaśnij jak przeprowadzić opisane w protokole obliczenia w czasie wielomianowym. Kto byłby stratny, gdyby wszyscy dysponowali nieograniczoną mocą obliczeniową?