Kryptografia

IIUWr.

1. (1pkt) Rozważ zmodyfikowany system Rabina, tj, taki, w kórym w skład klucza publicznego, oprócz n, wchodzi $B \in \langle 0, n-1\rangle$, a funkcja szyfrująca ma postać $E_{n,B}(x) = x(x+B) \bmod n$. Wyznacz funkcję deszyfrującą.

2. (1pkt) Załóżmy, że w systemie Rabina $p = 199$ $q = 211$ oraz $B = 1357$. Wykonaj następujące obliczenia:

   - Wyznacz cztery pierwiastki kwadratowe z 1 modulo $n = pq$;
   - Oblicz szyfrogram $y = E_{n,B}(32767)$;
   - Wyznacz cztery możliwe wyniki deszyfrowania y-ka.

3. (2pkt) Niech $y = x^2 \bmod p$ gdzie p jest liczbą pierwszą i znamy y. Istnieje prosty wzór pozwalający znaleźć x jeśli $p \equiv 3 \bmod 4$. Przypuśćmy, że jednak $p \equiv 1 \bmod 4$.

   (a) Pokaż, że losując u z Z_p^* mamy 50% szans na to, że $u^{p-1/2} \not\equiv 1 \bmod p$. Niech $p - 1 = 2^s t$, gdzie t jest liczbą nieparzystą. Pokaż, że $v = u^t \bmod p$ ma rząd 2^s w Z_p^*, czyli v jest pierwiastkiem pierwotnym stopnia 2^s z 1 modulo p.

   (b) Można wyliczyć $z = y^{(t+1)/2} \bmod p$ i $q = yz^{-2} \bmod p$. Pokaż, że $q^{2^{s-1}} \equiv 1 \bmod p$. Wprowadźmy oznaczenie $r = xz^{-1} \bmod p$. Pokaż, że $q = r^2 \bmod p$ i $r^{2^s} \equiv 1 \bmod p$. Pokaż też, że istnieje l takie, że $r = v^l \bmod p$.

   (c) Niech $l = l_0 + l_1 \cdot 2 + l_2 \cdot 2^2 + \cdots + l_{s-1} \cdot 2^{s-1}$. Pokaż, jak wyznaczyć $l_0, l_1, \ldots, l_{s-2}$ dysponując resztami y, q, v. (Wsk.: $l_0 = 0 \Leftrightarrow q^{2^{s-2}} \equiv 1 \bmod p$).

   (d) Pokaż, że x można wyliczyć ze wzoru $x = z \cdot r \bmod p = z \cdot v^l \bmod p$.

4. (1pkt) Jak wiadomo każda nieparzysta liczba naturalna n może być przedstawiona jako różnica kwadratów liczb naturalnych. Rozkład ten jest niejednoznaczny.

   - Pokaż, że jeśli $n = ab$ a liczby a i b są bliskie siebie, to istnieje taki rozkład na różnicę kwadratów, w którym jeden ze składników jest kwadratem małej liczby, z drugi - kwadratem liczby bliskiej $\sqrt{n}$.
   - Wykorzystaj ten fakt do sfaktoryzowania liczb: 8633, 809009, 92296873, 88169891. Zwróć uwagę, że efektywniej jest szukać kandydatów na większy kwadrat.
   - Ilu kandydatów sprawdzi Twoja metoda dla n mających czynnik różniący się od $\sqrt{n}$ o nie więcej niż $\sqrt[4]{n}$? Jeśli więcej niż jednego, to zweryfikuj ją.

5. (1pkt) Niech $n = 4633$. Użyj liczb 68, 152 i 153 oraz odpowiedniej bazy czynników, by rozłożyć n na czynniki. Jak wyglądają odpowiednie wektory? Pamiętaj, że do bazy czynników możesz włączyć liczbę -1.