KRYPTOGRAFIA, 2002 9.10.02

Lista nr 2

1. Jakie środki można przedsięwziąć by obronić się przed atakiem man-in-the-middle? Zaproponuj jakieś praktyczne rozwiązania w kontekście ustalania klucza między dwoma serwerami. Wskazówka: można korzystać z szyfrowania asymetrycznego.

2. Opracować protokół uzgadniania kluczy między dwoma serwerami, które często komunikują się ze sobą. Oczywiście można to zrobić przy pomocy protokołu Diffiego-Hellmana wykonywanego wielokrotnie. Chodzi jednak o to, by rozwiązanie było dużo efektywniejsze zarówno jeśli chodzi o wykonywane obliczenia jak i wolumen komunikacji.

3. Wyznaczyć wzór rekurencyjny na NWD(a, b) wynikający z Rozszerzonego Algorytmu Euklidesa.

4. Implementacja Algorytmu Euklidesa w oryginalnej postaci wymaga wykonywania dzieleń, co jest operacją dosyć kosztowną. Wymyślono lepszy algorytm, zwany *binary gcd*:

   INPUT: x, y, $x > y$
   OUTPUT: NWD(x, y)
   $g := 1$
   `while` x oraz y są parzyste
   $x := x/2$, $y := y/2$, $g := 2g$
   `while` $x \neq 0$
   `while` x parzyste `do` $x := x/2$
   `while` y parzyste `do` $y := y/2$
   $t := |x - y|/2$
   `if` $x \geq y$ `then` $x := t$ `else` $y := t$
   `return`$(g \cdot y)$

   Pokazać, że algorytm oblicza prawidłowo NWD. Przeanalizować jego złożoność obliczeniową i porównać z oryginalnym algorytmem.

5. Pokazać odwołując się do Chińskiego Twierdzenia o Resztach, że jeśli $n = pq$, $p \neq q$, oraz p i q są liczbami pierwszymi, to istnieją **dokładnie** cztery liczby $x < n$ takie że $x^2 = 1 \bmod n$. Zbadać ile istnieje pierwiastków z 1 modulo n dla n dowolnej postaci.

6. Pokazać, że jeśli jesteśmy w stanie wyznaczyć pierwiastki z 1 modulo n, to jesteśmy w stanie rozłożyć n na czynniki pierwsze.

7. Przyjmując, że koszt podnoszenia do kwadratu modulo n wynosi $\frac{3}{4}$ kosztu mnożenia modulo n wybrać w optymalny sposób podstawę, w której wyraża się wykładnik e w potęgowaniu $m^e \bmod n$ w metodzie iterowanego podnoszenia do kwadratu. Tzn. chodzi o taki wybór podstawy, by średnia złożoność obliczeniowa była jak najmniejsza. Założyć, że wszystkie operacje poza mnożeniem i podnoszeniem do kwadratu mają zaniedbywalny koszt.

/-/ Mirosław Kutyłowski