Algorytmiczne aspekty kryptografii, czerwiec 2007. Zadania z gwiazdką.

Zasady zaliczenia.

- Rozwiązania zadań należy przesyłać do **15 czewrca 2007, godz. 23:59**
  - zadania **1–6** oraz **Problem** na adres **niwinski@mimuw.edu.pl**
  - zadania **7–12** na adres **michal.strojnowski@gmail.com**

  w formacie **pdf** lub **ps**.
- Punkty z zadań przeliczane są bezpośrednio na ocenę z egzaminu.
- Zadania można rozwiązywać w **zespołach**, wtedy łączna liczba punktów dzieli się przez liczbę członków zespołu.
- Rozwiązanie powyższych zadań **nie** jest obowiązkowe. Zamiast tego można przystąpić do egzaminu indywidualnego.

Zadania

1. (**1 punkt**) Dowieść, ze funkcje jednokierunkowe nie mogą mieć obrazu wielomianowej wielkości. Dokładniej, jeśli f jest funkcją jednokierunkową (powiedzmy o dziedzinie $\{0,1\}^*$) a $p(n)$ dowolnym wielomianem, to dla dostatecznie dużych n, $|\{f(x) : |x| = n\}| > p(n)$.
2. (**2 punkty**) Wykazać, że jeśli istnieje funkcja jednokierunkowa, to istnieje również funkcja jednokierunkowa zachowująca długość.
3. (**1 punkt**) Zakładając, że funkcje jednokierunkowe istnieją, obalić następującą hipotezę:

   Dla każdej jednokierunkowej funkcji $f : \{0,1\}^* \to \{0,1\}^*$ zachowującej długość, funkcja
   $$f'(x) =_{def} f(x) \oplus x$$
   jest również jednokierunkowa, gdzie $\oplus$ oznacza *xor* po współrzędnych; np. $011 \oplus 110 = 101$.
4. (**2 punkty**) Przypuśćmy, że $f : \{0,1\}^* \to \{0,1\}^*$ jest jednokierunkowa, a ponadto różnowartościowa i zachowuje długość. Załóżmy ponadto, że $b(x)$ jest rdzeniem (ang. *hard core bit*) funkcji f i niech $\ell(n)$ będzie dowolnym wielomianem. Dowieść, że wówczas funkcja
   $$G(x) \;=\; b(f(x))\, b(f^2(x))\, b(f^3(x)) \ldots b(f^{\ell(|x|)}(x))$$
   jest generatorem pseudolosowym o współczynniku $\ell(n)$.

5. (**1 punkt**) Zakładamy, że G jest generatorem pseudolosowym, a h jest wielomianowo obliczalną permutacją (na słowach tej samej długości). Dowieść, że funkcje $G'(x) = h(G(x))$ i $G''(x) = G(h(x))$ są również generatorami pseudolosowymi.

6. (**1 punkt**) Wykazać, że gdybyśmy znali wielomianowy algorytm, który dla danych $\langle n, e, c = x^e \bmod n\rangle$ znajduje *pierwszy* bit x (gdzie $n = p \cdot q$, dla pewnych pierwszych p i q, $e \perp (p-1)\cdot(q-1)$, oraz $x \leq n$), to mielibyśmy również algorytm, który łamie RSA, tzn.

$$\langle n, e, c = x^e \bmod n\rangle \mapsto x.$$

   W powyższym pytaniu zakładamy, że x dane jest jako ciąg bitów długości $\lfloor \log n \rfloor + 1$ uzupełniony początkowymi zerami w razie potrzeby (dlatego pierwszy bit może być 0 lub 1).

7. (**2 punkty**) *Protokół Shamira podziału sekretu* polega na zaszyfrowaniu wiadomości M jako wartości $p(0)$ dla pewnego wielomianu p stopnia $t-1$ nad ciałem skończonym. Następnie n uczestnikom przekazywane są wartości tego wielomianu w punktach $1, 2, \ldots, n$. W ten sposób dowolny zbiór t graczy może interpolować ten wielomian i poznać M, a żadnen mniejszy zbiór graczy nie jest w stanie odtworzyć wielomianu. Metoda ta pozwala łatwo dodawać do siebie ukryte wiadomości: mając podzielony sekret M_1 i M_2, gracze mogą dodać do siebie wartości wielomianu, otrzymując podział sekretu $M_1 + M_2$. Pokaż jak za pomocą komunikacji pomiędzy graczami mogą oni uzyskać podział sekretu $M_1 \cdot M_2$, nie ujawniając w międzyczasie żadnemu z graczy wartości żadnego sekretu.

8. (**1 punkt**) Oznaczmy przez $S_X(a)$ podpis elektroniczny wiadomości a za pomocą klucza prywatnego X. Rozpatrzmy następujący protokół uzgadniania klucza pomiędzy A i B, oparty o protokół Diffiego-Hellmana:

   - A losuje x i wysyła do B parę $(g^x, S_A(g^x))$
   - B losuje y i wysyła do A parę $(g^y, S_B(g^y))$
   - Kluczem sesyjnym jest g^{xy}.

   Czy ten protokół jest odporny na atak *man-in-the-middle*? Odpowiedź uzasadnij.

9. (*M. Kutyłowski*, **3 punkty**) Poniżej opisany protokół ma zapewnić ustalenie klucza i potwierdzenie go. Oryginalny protokół został przepisany na listę niechlujnie z pewnymi "ulepszeniami". Należy lokalizować je i doprowadzić opis do porządnej postaci. W opisie A i B to uczesnicy protokołu, T to zaufana strona trzecia. $E_X(D)$ oznacza kyptogram utworzony przy pomocy klucza X z danych D. K_{XY} to wspólny klucz dla osób X i Y

   - A wybiera losowo r_A i do T wysyła A, B, r_A
   - T odsyła $E_{K_{AT}}(r_A, B, k)$
   - A wysyła do B kryptogram $E_{K_{BT}}(k)$
   - B deszyfruje ostatni kryptogram, wybiera losowo r_B i wysyła $E_k(r_B)$ do A

- A odpowiada za pomocą $E_k(r_A)$

Przedyskutować bezpieczeństwo opisanego wyżej schematu. Zaproponować poprawki. Uzasadnić dlaczego są odpowiednie.

10. (**1 punkt**) Dysponując odporną na kolizję funkcją kompresji $f : \Sigma^{n+r} \to \Sigma^n$ można utworzyć funkcję skrótu $h : \Sigma^* \to \Sigma^n$ w następujący sposób (*Schemat Merkle*)

    Dla wejścia $x \in \Sigma^*$:

    - Podziel x na t bloków $x_1, x_2, ..., x_t$, każdy o długości r bitów. W razie potrzeby, ostatni blok x_t należy uzupełnić zerami.
    - Przez b oznaczmy długość ciągu binarnego x. Utwórz dodatkowy blok x_{t+1} zawierający binarną reprezentację liczby b (zakładamy, że $b < 2^r$).
    - Niech $||$ oznacza konkatenację ciągów bitów. Oblicz wartości H_i według wzoru:
      - $H_0 = 0^n$
      - $H_i = f(H_{i-1}||x_i)$ dla $1 \leq i \leq t+1$
    - Wartością funkcji jest $h(x) = H_{t+1}$.

    Wykaż, że w tym schemacie znalezienie kolizji dla funkcji **skrótu** implikuje znalezienie kolizji dla funkcji **kompresji**[1]. Czy byłaby to prawda, gdyby pominąć dołączenie bloku x_{t+1}?

11. (**2 punkty**) Kwantowa teleportacja umożliwia przeniesienie stanu kwantowego w bezpieczny sposób, wykorzystując splątaną parę i klasyczny kanał komunikacji. Pokaż jak w analogiczny sposób, jeśli A i B dysponują elementami pary $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, to A może przekazać do B dwa bity informacji w bezpieczny sposób, wysyłając mu jeden kubit.

12. (*J. Talbot & D. Welsh*, **1 punkt**) Niech $n = pq$ będzie liczbą używaną do szyfrowania RSA, a p i q będą liczbami pierwszymi o takiej samej długości (w bitach). Pokaż, że jeśli iloczyn klucza prywatnego d i publicznego e spełnia nierówność $f = ed < n^{3/2}$, to istnieje algorytm wielomianowy faktoryzujący n, mając dane jedynie wartości n oraz f.

Problem (1–6 punktów) Spróbować znaleźć ogólnienie zadania 6 i podanego na wykładzie analogicznego faktu dla *ostatniego bitu*. Można na przykład zastanowić się nad i-tym bitem od początku lub od końca, gdzie i jest stałą lub funkcją od n. Można też podjąć taką hipotezę: Przypuśćmy, że $f : \{0,1\}^* \to \{0,1\}$ jest funkcją wielomianowo obliczalną także, że

$$|f^{-1}(\{0\}) \cap \{0,1\}^\ell| \approx |f^{-1}(\{1\}) \cap \{0,1\}^\ell|$$

[1] W pierwszej wersji funkcje skrótu i kompresji były w tym zdaniu omyłkowo zamienione. Podziękownie dla pana Jędrzeja Fulary za wykrycie pomyłki.

dla każdego ℓ. Czy gdybyśmy mieli algorytm

$$\langle n, e, c = x^e \bmod n \rangle \mapsto f(x)$$

to potrafilibyśmy łamać RSA ?

Część zadań wykorzystuje materiały Odeda Goldreicha.
Zadania podali Damian Niwiński i Michał Strojnowski.