Zkouška z předmětu MKR

Jméno a příjmení:

Příklad	1	2	3	4	Σ
Body					

Požadavky na vypracování

- Pište na bílé listy papíru formátu A4 a nepoužívejte obyčejnou tužkou ani červenou barvu.
- Každý příklad začněte na nové straně a dodržujte dělení jednotlivých příkladů na podúlohy.
- Kalkulačky jsou povoleny pro sčítání, násobení a umocňování modulo n (není-li uvedeno jinak). Ostatní výpočty musí být rozepsány krok za krokem. Penalisace: 50%.
- Každé své tvrzení řádně zdůvodněte. U výpočtů pište komentáře. Penalisace: 50%.

Příklady

1. [25 BODŮ] Šifrovací protokol RSA, útoky na RSA, problém faktorizace.
   (a) [10 BODŮ] Alice používá RSA šifrování s veřejným klíčem $(n, e) = (589, 23)$. Rozhodněte, zda některá z následujících dvojic (n, d) je Alicin soukromý klíč: $(589, 45)$, $(589, 47)$, $(589, 49)$. Alice obdržela zprávu $b = 10$, dešifrujte tuto zprávu.
   (b) [10 BODŮ] Je znám veřejný i soukromý klíč jednoho z účastníků protokolu RSA, $(n, e) = (7811, 17)$, $(n, d) = (7811, 449)$. Použijte útok insidera k faktorizaci modulu $n = 7811$. (Pozn.: Nejedná se o faktorizaci hrubou silou, nýbrž o faktorizaci na základě znalosti násobku $\varphi(n)$!)
   (c) [5 BODŮ] Dokažte, že znalost $\varphi(n)$ umožní faktorizovat modul n protokolu RSA.
2. [25 BODŮ] Diffieho-Hellmanova domluva klíče, šifrovací protokol ElGamal, problém diskrétního logaritmu.
   (a) [5 BODŮ] Ověřte, že prvek $a = 124$ je generátorem cyklické grupy $\mathbb{Z}^*_{131}$.
   (b) [10 BODŮ] Algoritmem Baby step-Giant step spočtěte $\mathrm{dlog}_{124}(90)$ v grupě $\mathbb{Z}^*_{131}$.
   (c) [10 BODŮ] ElGamalův šifrovací protokol používá cyklickou grupou $\mathbb{Z}^*_{131}$ s generátorem $a = 124$. Alicin veřejný klíč je $e = 90$. Alice dostala zprávu $(c, \bar{m}) = (73, 103)$, dešifrujte tuto zprávu.
3. [25 BODŮ] Testy prvočíselnosti, generování náhodných prvočísel.
   (a) [5 BODŮ] Fermatovým testem ověřte, zda je číslo $n = 377$ prvočíslo. Použijte k tomu dva svědky: $a = 12$, $b = 52$.
   (b) [5 BODŮ] Kdy lze pomocí prvku, který dosvědčuje neprvočíselnost čísla n u Fermatova testu, faktorizovat číslo n? Využijte výpočtů z předchozí podotázky a faktorizujte $n = 377$.
   (c) [10 BODŮ] Nalezněte množinu všech falešných svědků prvočíselnosti u Fermatova testu pro $n = 377$.
   (d) [5 BODŮ] Prozradí svědek $a = 12$ neprvočíselnost čísla $n = 377$, použijete-li Millerův-Rabinův test?
4. [25 BODŮ] Subexponenciální algoritmy na faktorizaci a diskrétní logaritmus.
   (a) [5 BODŮ] V grupě $\mathbb{Z}^*_{19}$ známe representaci $(s, t) = (6, 8)$ prvku 1 vzhledem ke generátoru $a = 2$ a prvku $b = 7$. Spočtěte $\mathrm{dlog}_2(7)$ v $\mathbb{Z}^*_{19}$.
   (b) [15 BODŮ] Je dána cyklická podgrupa G s generátorem $a = 16$ řádu $q = 37$ v grupě $\mathbb{Z}^*_{149}$. Algoritmem SEDL spočtěte $\mathrm{dlog}_{16}(36)$ v grupě G, volte parametr hladkosti $y = 3$.
   (c) [5 BODŮ] Nechť $G = \langle a \rangle$ je podgrupa řádu q v grupě $\mathbb{Z}^*_p$, kde p je prvočíslo. Dokažte, že $\mathrm{dlog}_a(b)$ je definován, právě když $b^q = 1$ v $\mathbb{Z}^*_p$.

`DD-MM-RRRR: písemný test z MKR`