Zkouška z předmětu MKR

Jméno a příjmení:

Příklad	Body
1	
2	
3	
4	
Σ	

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 v $\mathbb{Z}_n$. Pro ostatní výpočty použijte algoritmy známé z přednášky. Výpočet hrubou silou nebo uhodnutí řešení bude bodováno nula body.
- Každé své tvrzení řádně zdůvodněte. U výpočtů pište komentáře. Penalisace: 50%.

Příklady

1. [25 BODŮ] Šifrovací protokol RSA, útoky na RSA, problém faktorizace.
   (a) [5 BODŮ] Alice používá RSA šifrování s veřejným klíčem $(n, e) = (589, 23)$. Rozhodněte, zda některá z následujících dvojic (n, d) je Alicin soukromý klíč: $(589, 45)$, $(589, 47)$, $(589, 49)$.
   (b) [15 BODŮ] Je znám veřejný i soukromý klíč jednoho z účastníků protokolu RSA, $(n, e) = (851, 13)$, $(n, d) = (851, 61)$. Použijte útok insidera k faktorizaci modulu $n = 851$. (Pro umocňování zde použijte metodu opakovaných čtverců.) 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) [15 BODŮ] Je dána cyklická grupa $\mathbb{Z}^*_{131}$ s generátorem $a = 124$, kde 131 je prvočíslo. Algoritmem Baby step-Giant step spočtěte $\mathrm{dlog}_{124}(90)$ v $\mathbb{Z}^*_{131}$. (Inverzní prvek zde spočtěte pomocí rozšířeného Eukleidova algoritmu.)
   (b) [10 BODŮ] ElGamalův šifrovací protokol používá 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 (využijte výpočtů z předchozí části).
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) [15 BODŮ] Nalezněte množinu všech falešných svědků prvočíselnosti u Fermatova testu pro $n = 377$. (Použijte Čínskou větu o zbytcích a v cyklických grupách řešte rovnici přes generátor grupy.)
4. [25 BODŮ] Subexponenciální algoritmy na faktorizaci a diskrétní logaritmus.
   (a) [20 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 $y = 5$.
   Pro první fázi algoritmu si vyberte dostatečný počet použitelných rovností z následující nabídky. V $\mathbb{Z}_{149}$ platí: $16^7 \cdot 36^8 \cdot (-1) = 144$, $16^9 \cdot 36^{10} \cdot (-1) = 86$, $16^4 \cdot 36^8 \cdot 1 = 96$, $16^{15} \cdot 36^3 \cdot 44 = 40$, $16^9 \cdot 36^6 \cdot (-1) = 45$, $16^4 \cdot 36^7 \cdot 22 = 9$. Svůj vývěr zdůvodněte.
   (b) [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`