15. detsember 2005

1. **(15 punkti)** Olgu meil antud rühm G, kus Diffie-Hellmani ülesanne on raske, olgu $|G| = m$ ja olgu g selle rühma mingi moodustaja. Olgu meil ka teada Alice'i ElGamali krüptosüsteemi avalik võti $h = g^a$ (a ei ole teada). Olgu $m \in G$. Me moodustame m-st Alice'i avaliku võtmega kaks erinevat krüptoteksti g^r, mh^r) ja $(g^{r'}, mh^{r'})$ ning avalikustame need. Kuidas me saame Bob'ile tõestada, et need kaks krüptoteksti vastavad tõepoolest samale avatekstile, avalikustamata seejuures teadet m?

2. **(10 punkti)** Vaatame järgmist identifitseerimisskeemi. Alice genereerib RSA mooduli $n = pq$. Alice'i avalik võti on n, salajane võti on (p, q). Kui Alice soovib end Bobile identifitseerida, siis genereerib Bob juhusliku ruutjäägi $x \in \mathbb{Z}_n$ ja saadab selle Alice'ile. Alice leiab sellise $y \in \mathbb{Z}_n$, et $y^2 \equiv x \pmod{n}$, ja saadab selle tagasi. Bob kontrollib, et $y^2 \equiv x \pmod{n}$ ja loeb Alice'i identifitseerituks, kui see tõepoolest nii on. Miks on see skeem ebaturvaline?

3. **(10 punkti)** Olgu E mingi plokkšifri šifreerimisfunktsioon, s.t. $E_a(b)$ šifreerib avateksti b võtmega a. Olgu nii võtmete kui ka avatekstide pikkus n. Vaatame kompressioonifunktsiooni $h(x_1, x_2) = E_{x_1 \oplus x_2}(x_2) \oplus x_1 \oplus x_2$, kus x_1 ja x_2 on bitijadad pikkusega n. Näita, kuidas leida funktsiooni h kollisioone, kui me võime välja kutsuda E-d ja dešifreerimisfunktsiooni D meie valitud argumentidel.

4. **(5+10 punkti)** Seljakotiülesande raskusel põhineva signatuuriskeemi võib püüda luua järgmiselt. Olgu n signeeritavate teadete pikkus ($n \approx 200$). Olgu p n-bitine algarv. Olgu $E = (e_{ij})$ maatriks suurusega $n \times 2n$, kus $e_{ij} \in \{0, 1\}$ ja E vasakpoolne alammaatriks suurusega $n \times n$ on pööratav $\mathbb{Z}_p$-s. Olgu $a_{n+1}, \ldots, a_{2n}$ juhuslikud n-bitised arvud. Olgu $a_1, \ldots, a_n \in \mathbb{Z}_p$ sellised, et $2^{i-1} \equiv \sum_{j=1}^{2n} e_{ij} a_j \pmod{p}$ kehtiks iga $i \in \{1, \ldots, n\}$ jaoks (nad on üheselt määratud). Verifitseerimisvõti on $(n, p, a_1, \ldots, a_{2n})$. Signeerimisvõti on E.
Teate $m = b_1 \cdots b_n$ signatuuriks on arvujada $(\varepsilon_1, \ldots, \varepsilon_{2n})$, kus $\varepsilon_j = \sum_{i=1}^{n} e_{ij} b_i$ $(1 \leqslant j \leqslant 2n)$. Kui on antud teade $b_1 \cdots b_n$ ja signatuur $(\varepsilon_1, \ldots, \varepsilon_{2n})$, siis aktsepteeritakse signatuur juhul, kui $0 \leqslant \varepsilon_i \leqslant n$ iga i jaoks, ning $\sum_{i=1}^{n} b_i 2^{i-1} \equiv \sum_{j=1}^{2n} \varepsilon_j a_j \pmod{p}$. Näita, et antud signatuuriskeem töötab. Miks ei ole see skeem turvaline?

5. **(15 punkti)** Vaatame järgmist kompressioonifunktsiooni h. Olgu $n = pq$, kus $p = 2p' + 1$, $q = 2q' + 1$ ning p, q, p' ja q' on kõik suured algarvud. Olgu $g \in \mathbb{Z}_n^*$ järk $2p'q'$ (see on $\mathbb{Z}_n^*$ elementide maksimaalne võimalik järk). Olgu n ja g genereerijaks mingi usaldatud osapool, kes ei avalda suurusi p, p', q, q'. Olgu $h : \mathbb{Z}_{n^2} \to \mathbb{Z}_n$ defineeritud järgmiselt: $h(x) = g^x \bmod n$. Näita, et h on kollisioonikindel.
Vihje: Tuleta meelde, kuidas tegurdada RSA moodulit n, kui on antud teineteisele vastavad avalik astendaja e ja salajane astendaja d.

6. **(10 punkti)** Vaatame kõige lihtsamat RSA signatuuriskeemi, s.t. $n = pq$ on RSA moodul, $e \in \mathbb{Z}_{\varphi(n)}^*$, $d = e^{-1} \pmod{\varphi(n)}$, signeerimisvõti on (n, d), verifitseerimisvõti on (n, e), $sig_{(n,d)}(m) = m^d \bmod n$ ja $ver_{(n,e)}(m, s) = [s^e \equiv m \pmod{n}]$. Teadku me n-i ja e-d, kuid ärgu teadku p-d, q-d ega d-d. Me soovime leida signatuuri teatele $m \in \mathbb{Z}_n$. Meil on ligipääs oraaklile $\mathcal{O}$, mis sisendi x korral tagastab $x^d \bmod n$, kuid ainult juhul, kui $x \in X \subseteq \mathbb{Z}_n$, kus X on mingi fikseeritud alamhulk, mille jaoks kontroll $x \in X$ on lihtne ning $|X| \approx n/100$. Kirjelda, kuidas $\mathcal{O}$-d kasutades leida signatuur m-le.

7. **(4+2+2 punkti)** Olgu $a, b, c \in \mathbb{Z}_n^*$. Vaatame kompressioonifunktsiooni $h(x_1, x_2) = ax_1x_2 + bx_1 + cx_2$, kus $x_1, x_2 \in \mathbb{Z}_n$ ja kõik arvutused toimuvad $\mathbb{Z}_n$-s. Hinda selle funktsiooni kindlust originaali leidmise suhtes, kindlust teise originaali leidmise suhtes ja kollisioonikindlust.

Töö eest saab ülimalt 40 punkti. Materjalide kasutamine on lubatud.

December 15th, 2005

1. **(15 points)** Let G be a group with hard Diffie-Hellman problem. Let $m = |G|$ and g be a generator of G. Let Alice's public key for the ElGamal encryption system be $h = g^a$ where a is unknown to us. We use h to create two encryptions of a message m — (g^r, mh^r) and $(g^{r'}, mh^{r'})$. How can we prove to Bob that these two cryptotexts indeed correspond to the same plaintext without revealing m?

2. **(10 points)** Consider the following identification scheme. Alice generates an RSA modulus $n = pq$, publishes n and keeps (p, q) secret. When Alice wants to identify herself to Bob, Bob generates a random quadratic residue $x \in \mathbb{Z}_n$ and sends it to Alice. Alice responds with an $y \in \mathbb{Z}_n$, such that $y^2 \equiv x \pmod{n}$. Bob verifies whether this holds and accepts if it does. Why is this scheme insecure?

3. **(10 points)** Let E be the encryption function of some block cipher, i.e. $E_a(b)$ encrypts the plaintext b with the key a. Let the length of keys and plaintexts be n. Consider the compression function $h(x_1, x_2) = E_{x_1 \oplus x_2}(x_2) \oplus x_1 \oplus x_2$ where x_1 and x_2 are n-bit strings. How to find the collisions of h if we may invoke E and the decryption function D on the arguments of our choice?

4. **(5+10 points)** A signature scheme based on the knapsack problem may be constructed as follows. Let n be the length of signed messages ($n \approx 200$). Let p be a n-bit prime. Let $E = (e_{ij})$ be a matrix of size $n \times 2n$, such that $e_{ij} \in \{0, 1\}$ and the left submatrix of E of size $n \times n$ is invertible in $\mathbb{Z}_p$. Let $a_{n+1}, \ldots, a_{2n}$ random n-bit numbers and let $a_1, \ldots, a_n \in \mathbb{Z}_p$ be such that $2^{i-1} \equiv \sum_{j=1}^{2n} e_{ij} a_j \pmod{p}$ holds for all $i \in \{1, \ldots, n\}$ (the numbers $a_1, \ldots, a_n$ are uniquely determined). The verification key is $(n, p, a_1, \ldots, a_{2n})$. The signature key is E.
The signature of a message $m = b_1 \cdots b_n$ is a sequence $(\varepsilon_1, \ldots, \varepsilon_{2n})$ where $\varepsilon_j = \sum_{i=1}^{n} e_{ij} b_i$ for all $j \in \{1, \ldots, 2n\}$. To verify a signature $(\varepsilon_1, \ldots, \varepsilon_{2n})$ for the message $b_1 \cdots b_n$ one checks that $0 \leqslant \varepsilon_i \leqslant n$ for all i and $\sum_{i=1}^{n} b_i 2^{i-1} \equiv \sum_{j=1}^{2n} \varepsilon_j a_j \pmod{p}$. Show that the scheme works. Why is it insecure?

5. **(15 points)** Consider the following compression function h. Let $n = pq$, $p = 2p' + 1$, $q = 2q' + 1$, and p, q, p', q' are all large prime numbers. Let the order of $g \in \mathbb{Z}_n^*$ be $2p'q'$ (the maximum possible order of the elements of $\mathbb{Z}_n^*$). Let n and g be generated by some trusted party that does not reveal p, q, p', q'. Let $h : \mathbb{Z}_{n^2} \to \mathbb{Z}_n$ be defined by $h(x) = g^x \bmod n$. Show that h is collision-resistant.
Hint: Recall how to factor an RSA modulus n if we know the corresponding public exponent e and secret exponent d.

6. **(10 points)** Consider the simplest RSA signature scheme, i.e. $n = pq$ is an RSA modulus, $e \in \mathbb{Z}_{\varphi(n)}^*$, $d = e^{-1} \pmod{\varphi(n)}$, signature key is (n, d), verification key is (n, e), $sig_{(n,d)}(m) = m^d \bmod n$ and $ver_{(n,e)}(m, s) = [s^e \equiv m \pmod{n}]$. Let n and e be known to us, let p, q, d be unknown. We want to sign a message $m \in \mathbb{Z}_n$. We have access to an oracle $\mathcal{O}$ that on input x returns $x^d \bmod n$, but only if $x \in X \subseteq \mathbb{Z}_n$, where X is some fixed subset whose membership problem is easy and whose cardinality is about $n/100$. Describe how to sign m with the help of $\mathcal{O}$.

7. **(4+2+2 points)** Let $a, b, c \in \mathbb{Z}_n^*$. Consider the compression function $h(x_1, x_2) = ax_1x_2 + bx_1 + cx_2$ where $x_1, x_2 \in \mathbb{Z}_n$ and all computations are done in $\mathbb{Z}_n$. Judge the preimage resistance, second preimage resistance, and collision resistance of that function.

At most 40 points can be obtained. The usage of notes is permitted.