Cryptology I exam

15. january 2008

1. We could try to develop a signature scheme based on the security of the knapsack problem. Let n be the length of the signed messages ($n \approx 200$). Let p be an n-bit prime and let $E = (e_{ij})$ be a matrix of size $n \times 2n$, where $e_{ij} \in \{0, 1\}$ and the left submatrix of size $n \times n$ is invertible in $\mathbb{Z}_p$. 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 $i \in \{1, \ldots, n\}$ (note that this determines them uniquely) and let $a_{n+1}, \ldots, a_{2n}$ be random n-bit numbers. The verification key is $(n, p, a_1, \ldots, a_{2n})$ and the signing key is E.
   The signature of a message $m = b_1 \cdots b_n$ is a string of numbers $(\varepsilon_1, \ldots, \varepsilon_{2n})$ where $\varepsilon_j = \sum_{i=1}^{n} e_{ij} b_i$ $(1 \leqslant j \leqslant 2n)$. If we are given a message $b_1 \cdots b_n$ and a signature $(\varepsilon_1, \ldots, \varepsilon_{2n})$, the signature is accepted iff $0 \leqslant \varepsilon_i \leqslant n$ 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 given signature scheme is functional. Why isn't it secure?

2. Let E be the encryption function of some block chipher, so $E_a(b)$ encrypts the plaintext b with the key a. Let the length of both keys and plaintexts be n bits. Let us consider a 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 bitstrings of length b. Show how to find collisions for h if we can call both E and the decryption function D corresponding to it on all the arguments of our choice.

3. Let $\mathbf{X}$ and $\mathbf{Y}$ be random variables over the ring $\mathbb{Z}_n$ and let $\mathbf{Z} = \mathbf{X} + \mathbf{Y}$. Show that $H(\mathbf{Z}|\mathbf{X}) = H(\mathbf{Y}|\mathbf{X})$ and that if $\mathbf{X}$ and $\mathbf{Y}$ are independent then $H(\mathbf{X}) \leqslant H(\mathbf{Z})$.

4. What are Zero-knowledge proofs?

5. What does it mean for a block cipher to be pseudorandom. Why do we get a cryptosystem semantically secure against chosen plaintext attacks if we use a pseudorandom permutation in the CTR-mode?

6. Let n be some 1024-bit RSA modulus and let $e = 3$ be the public exponent. Assume that the secret exponent d is unknown. Let c be an RSA cryptotext created with the public key (n, e). How to find the plaintext m corresponding to c if we know that $1 \leqslant m \leqslant 10^{40}$?

Exam makes up one third of the final grade.
All the exam problems are of equal weight.