Final exam in Cryptology I
November 9th, 2009

1. Let (n, e) be Alice's public key for the RSA encryption system. Let n be a rather long modulus (say, 2048 bits) and let e be long, too (chosen randomly from $\mathbb{Z}^*_{\varphi(n)}$). Let $c = k^e \bmod n$ be the encryption of a DES key k that has been sent to Alice. Here k is a bitstring of length 56 that we naturally interpret as an integer between 0 and $2^{56} - 1$.

   Suppose Eve has learned c and wants to learn k, but performing a brute-force search (up to 2^{56} modular exponentiations) is somewhat beyond her computational capabilities. However, Eve has learned that the sought-after number k is actually a product of two 28-bit numbers. Show how she can find k.

2. Construct a signature scheme with the following parameters:

   - There is a public RSA modulus $n = pq$. Nobody knows the factors p and q.
   - There is a (public) collision-resistant hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_n$.
   - The secret key of a party is a randomly chosen element $s \in \mathbb{Z}^*_n$.
   - The corresponding public key is $k = s^2 \bmod n$.
   - The signature of a message $m \in \{0,1\}^*$ is (x, y), where $x, y \in \mathbb{Z}_n$.
   - The verification algorithm checks that $x^2 - ky^2 = H(m)$.

   I.e. explain how the signing procedure works.
   Informal remark. The scheme is actually insecure. It is possible to find x and y without knowing s.

3. Let H_1 and H_2 be two hash functions where H_2 is collision-resistant, but H_1 is not. What can be said about the collision-resistance of H where $H(x) = H_1(H_2(x))$?

4. From an identification protocol consisting of three messages (commitment C, challenge k and response $r(C, k)$) it is possible to construct a signature scheme, where the signature of a message m is $(C, r(C, h(C, m)))$. Work out the details for the Okamoto identification protocol (explain what are the secret and public keys, how do signing and verification algorithms work).

The test makes up a quarter of the final grade.
All exercises in the test have equal weight.