KTH Computer Science
and Communication

Homework II, Foundations of Cryptography 2007

Due on March 7 at 13.15. The general rules on homework solutions available at the course home-page apply. In particular discussion of ideas up to groups of three people are allowed but implementation should be done individually. In this problem set you are allowed to use premade subroutines to handle some aspects of large number arithmetic. You are allowed to use routines for addition, subtraction, and multiplication. You are not allowed to use more sophisticated routines solve operations such as modular reduction, modular division or primality. Whenever in doubt ask Johan. This time one bonus questions for those interested.

1 (20p) Let P be your personal number (a 10 digit number). I want you to solve the discrete logarithm problem for P with $g = 2$ modulo a prime q, i.e. to find x such that $2^x = P \bmod q$. You may use $q1 = 786443737115847721467979$ or $q2 = 31095089927221660763$ both available on course homepage.

2 (20p) Let SHA-1k be a truncated variant of SHA-1 where each of the words used is a k bit integer instead of the designed 32 bit integers. All constants are truncated to the least k significant bits and the basic round function maps $16k$ bits to $5k$ bits. Replace the left shift of 30 by a right shift of 2 keeping all the other operations. Find a collision for this round function. Use as large a value of k as possible. Your score for a correct solution is $\min(4 \cdot (k-8), 20)$. In other words solutions for $k > 13$ do not automatically give extra points but 40 points are distributed equally among the students solving the largest value of k[1]. The implementation will not be checked against a reference implementation and any implementation that is close enough to give "essentially" SHA-behavior is accepted.

3 (15p) You are given a collision resistant hash function function $h : \{0,1\}^{2m} \mapsto \{0,1\}^m$ for some m. You want to use this to construct a hash function h' which takes as inputs messages whose bit lengths are positive multiples of m. You try the following where $|x|$ denote the bit length of x.

- If $|x| = m$, then $h'(x) = x$.
- If $|x| = 2m$, then $h'(x) = h(x)$.
- Suppose $|x| = sm$ with $s > 2$ then if s is even let $t = s/2$ and if it is odd set $t = (s+1)/2$. Let x_1 be the first t m-bit blocks of x and x_2 the rest. Set $h'(x) = h(h'(x_1)||h'(x_2))$ where "||" denotes concatenation.

3a (5p) Is h' a collision resistant hash function?

3b (5p) Is h' a collision resistant hash function if we restrict to inputs of a fixed length?

[1] Only solutions handed in on time count with respect to this competition.

3c (5p) Is h' a collision resistant hash function if we restrict to inputs of a fixed length and this length is a power of 2?

In each case you should present either an efficient way to construct a collision for h' or a proof that if you find a collision for h' then you can also find a collision for h and since we assumed h to be collision resistant we can conclude that also h' is collision resistant.

4 (15p) Find a prime p with at least 1023 bits such that it is of the form $p = 1 + 2q$ where q is also prime and such that the first 10 digits of p give the digits of your personal number.

5 (15p) An elliptic curve

$$y^2 = x^3 + ax + b$$

is said to be singular if $4a^3 + 27b^2 = 0$. Let us study this condition.

5a (9p) Study the elliptic curves defined by

$$y^2 \equiv x^3 + 2x + b \bmod 7$$

by hand for $b = 4$ and $b = 5$. Calculate all points and a complete addition table according to the formulas given in the book. Can you tell any significant difference between the two cases?

5b (6p) Draw the curve

$$y^2 = x^3 - 3x + 2$$

over the real numbers. For which pairs of points does our geometric definition of the group operation work? Can you explain what goes wrong?

6 (15p) In the Digital Signature Standard where the public key is given by p, g and y where $p = 1 + tq$, p and q are primes and g is a generator of the subgroup of order q mod p. The secret key is x where $g^x \equiv y$ mod p and we also have a public, cryptographically strong hash function h. A signature of a message M is given by (r, s) where

$$\begin{aligned} r &\equiv (g^k \bmod p) \bmod q \\ s &\equiv k^{-1}(h(M) + xr) \bmod q \end{aligned}$$

where k is supposed to be chosen as a fresh random number each time. A smart(?) programmer decided to save energy by storing a randomly chosen k_0 and then using $k = k_0 + h(i) \cdot 4711$ for the i'th signature. It might also be the case that the user signs the same message many times. Could either of these circumstances make it possible for an attacker to reconstruct the secret key? Discuss both the case where only the special values of k are used and the case where this construction is used with together with the procedure where the same M is signed many times.

7 (Bonus problem) (20p) Let me first state some background that you may prove, consult a book to confirm or simply take on faith. Solving the equations $x^2 \equiv a \bmod m$ is, computationally easy if m is a prime but if m is composite it is a computational problem that is essentially equivalent to factoring m.

Consider the following protocol where P proves to V that he knows a solution x_0 to $x^2 \equiv a \bmod m$ where we assume that $GCD(a, m) = 1$.

1. P picks a random number y, $0 < y < m$ such that $GCD(y, m) = 1$ and sends $\alpha = y^2 \bmod m$ to V.
2. V picks a random $b \in \{0, 1\}$ and sends to P.
3. If $b = 0$, P sends $\beta = y$ to V and otherwise P sends $\beta = x_0 y \bmod m$.
4. If $b = 0$, V checks that $\beta^2 = \alpha \bmod m$ and if $b = 1$ V checks $\beta^2 = a\alpha \bmod m$.

To what extent is this protocol complete (P who knows a solution x_0 succeeds), sound (P who does not know a solution x_0 fails), and zero-knowledge (V gets no information about x_0)?

As stated above the ability to extract square-roots modulo m is equivalent to knowing the factorization of m. Consider the following protocol allowing P to prove that he knows the factorization of m.

1. V picks a random number z, $0 < z < m$ such that $GCD(z, m) = 1$ and sends $\gamma = z^2 \bmod m$ to P.
2. P returns a solution to $x^2 = \gamma \bmod m$.

Is this protocol complete, sound, zero-knowledge? Consider zero-knowledge both with respect to V and with respect to a listener.

Suppose we replace the second step in this second protocol by P proving (using the first protocol) that he knows a solution to the given equation? Again you should study completeness, soundness and zero-knowledge.