Cryptography Tutorial 5 (15,16-10-2014)
Public-key cryptosystems

1. **Diffie-Hellman** Perform in detail all steps of Diffie Hellman protocol with $p = 223, q = 2, x = 25, y = 13$.

   Solution. $X = 2^{25} \mod 223 = 68, Y = 2^{13} \mod 223 = 164, K = X^{13} = Y^{25} = 196$. Discuss the hardness of logarithm and the diffie-hellman problem of computing q^{xy} from q^x and q^y.

2. **Knapsack.** Suppose that Alice wants to send a message $w = 011101$ to Bob using the Knapsack cryptosystem with $X - (2, 4, 7, 17, 31, 70), m - 145$ and $u - 42$.

   Solution.

   (a) $x'_i = ux_i \mod m$. Therefore $X' = (84, 23, 4, 134, 142, 40)$.

   (b) $c = X'w^t = 23 + 4 + 134 + 40 = 56 \mod 145$.

   (c) $c' = u^{-1}c = 38 * 56 = 98 \mod 145$. Solving knapsack with superincreasing is easy just take the ighest number that does not exceed the target (98). This gives us back $w = 011101$.

3. Suppose that we use a RSA cryptosystems with $p = 41$, $q = 83$ and $d = 857$. Try to find out e and encrypt the plaintexts "security".

   (Hint: Modular Arithmetic Calculator: `http://ptrow.com/perl/calculator.pl`)

   Solution. $n = pq = 3403$, $\phi(n) = (p-1)(q-1) = 3280$. Since $e = d^{-1} \mod \phi(n)$, we can get $e = 953$. Since $10^3 < 3403 < 10^4$, we should divided the plaintext into blocks of length 3.

   "security" $\to$ 18 04 02 20 17 08 19 24 = 180 402 201 708 819 24

   The cryptotexts are 242 2152 18 116 450 801.

4. (**Mersenne prime**) Prove the following facts.

   (a) If $2^p - 1$ is prime, then p is a prime.

   (b) If $a^n - 1$ is prime, then a is 2 and n is prime.

   Solution.

   (a) Let r and s be positive integers, then the polynomial

   $$x^{rs} - 1 = (x^s - 1) \times (x^{s(r-1)} + x^{s(r-2)} + \cdots + x^s + 1).$$

   So if n is composite (say $r.s$ with $1 < s < n$), then $2^n - 1$ is also composite (because it is divisible by $2^s - 1$).

   (b) Notice that we can say more: suppose $n > 1$. Since $x - 1$ divides $x^n - 1$, for the latter to be prime the former must be one. This gives the following.

5. Suppose that we know $p - q$ is small and $n = pq = 549077$, try to factorize n.

   Solution.

Since $\sqrt{549077} \approx 740$, then we try $741^2 - 549077 = 4$. Therefore $p = 741 + 2 = 743$ and $q = 741 - 2 = 739$. $549077 = 739 \times 743$.

Ex:Try to factorize 2021.

6. Suppose Alice is sending the same message m to Bob, Charlie and Dave, who have the following public RSA keys: $(3, 377)(3, 391)(3, 589)$. The encryptions of the message are $330, 34$ and 419 respectively. Without factorization find m.

   Solution. We want to solve the following

$$
\begin{aligned}
c &\equiv 330 && \text{mod } 377 \\
c &\equiv 34 && \text{mod } 391 \\
c &\equiv 419 && \text{mod } 589
\end{aligned}
$$

   This can be done by Chinese remainder theorem! We obtain 1061208 and by computing it's 3rd root we get 102. Note that broadcast to three players are necessary. The reason for this is that the message m has to be lower than all three moduli, therefore $m^3 < 377 * 391 * 589$, allowing us to use integer third root at the end of the attack.