T-79.5501 Cryptology Spring 2009

Homework 8

Tutor : Joo Y. Cho
joo.cho@tkk.fi

2nd April 2009

Q1. Test the primality of 2009 using

1. the Solovay-Strassen test with $a = 442$
2. the Miller-Rabin test with $a = 442$.

A1-a). (The Solovay-Strassen test)
We proceed as written in the lecture slides. We have $n = 2009$, $a = 442 = 2 \cdot 13 \cdot 17$.

$$\left(\frac{442}{2009}\right) = \left(\frac{2}{2009}\right)\left(\frac{13}{2009}\right)\left(\frac{17}{2009}\right) = \left(\frac{13}{2009}\right)\left(\frac{17}{2009}\right)$$
$$= \left(\frac{7}{13}\right)\left(\frac{3}{17}\right) = \left(\frac{6}{7}\right)\left(\frac{2}{3}\right) = -\left(\frac{3}{7}\right) = 1$$

Also, we compute $442^{\frac{n-1}{2}} = 442^{1004} \bmod 2009$. Since $442^4 \equiv 1 \bmod 2009$, we get $442^{1004} = 442^{4\cdot 251} \equiv 1 \bmod 2009$.
Hence, $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}$ so n is prime.

A1-b). (The Miller-Rabin test) We have $n = 2009$, $a = 442$, $n - 1 = 2^3 \cdot 251$ and $k = 3$.

- $b \leftarrow 442^{251} \mod 2009 = 50$ by square-and-multiply.
- $b \not\equiv 1 \mod n$, continue.
- $i = 0$: $b \not\equiv -1 \pmod{n}$, $b \leftarrow b^2 = 491$.
- $i = 1$: $b \not\equiv -1 \pmod{n}$, $b \leftarrow b^2 = 1$.
- $i = 2$: $b \not\equiv -1 \pmod{n}$, $b \leftarrow b^2 = 1$.
- Answer: “n is composite”.

Q2.

1. Find all square roots of 1 modulo $4453 = 61 \cdot 73$.
2. 2777 is a square root of 3586 modulo 4453. Find all square roots of 3586 modulo 4453.

A2-a). The task is to find x such that $x^2 \equiv 1 \bmod 4453$.

- It is obvious that $x = \pm 1$ are square roots.
- Also, we have

$$\begin{aligned} x &\equiv -1 (\mathrm{mod} 61) \\ x &\equiv 1 (\mathrm{mod} 73). \end{aligned}$$

  We get $61^{-1} \equiv 6 \bmod 73$ and $73^{-1} \equiv 56 \bmod 61$.
- Using CRT, we get $x = -1 \cdot 73 \cdot 56 + 1 \cdot 61 \cdot 6 \equiv 731 \bmod 4453$.
- In a similar way, we can get $x = -731$. Hence, ± 1 and ± 731 are four square roots of $1 \mod 4453$.

A2-b). From the lecture slides,

- ± 1 and ± 731 are the square roots of 1 mod n. Put $w = 731$.
- Given a square root b of a, the four square roots of $a \mod n$ are $\pm b$ and $\pm bw$.
- So with $a = 3586$, $b = 2777$, $n = 4453$, $w = 731$, the four square roots of $3586 \mod 4453$ are ± 2777 and $\pm 2777 \cdot 731$, namely, $\{2777, 1676, 3872, 581\}$.

Q3. (Stinson 5.24) Suppose that $i \geq 2$ and $b^2 \equiv a \pmod{p^{i-1}}$. it was shown that there is a unique $x \in \mathbf{Z}_{p^i}$, such that $x^2 \equiv a \pmod{p^i}$ and $x \equiv b \pmod{p^{i-1}}$ and

$$
\begin{aligned}
b^2 &= a + mp^{i-1} \bmod p^i && (1)\\
x &= b + np^{i-1} \bmod p^i && (2)\\
n &= \frac{p-1}{2} b^{-1} m \bmod p. && (3)
\end{aligned}
$$

Starting with the congruence $6^2 \equiv 17 \pmod{19}$, find square roots of 17 modulo 19^2.

A3. We have $b^2 \equiv a \pmod{p^{i-1}}$, $x^2 \equiv a \pmod{p^i}$ and $x \equiv b \pmod{p^{i-1}}$.

$$\begin{aligned} b^2 &= a + mp^{i-1} \bmod p^i \\ x &= b + np^{i-1} \bmod p^i \\ n &= \frac{p-1}{2} b^{-1} m \bmod p. \end{aligned}$$

Using these equations, we find square roots of 17 modulo 19^2 and modulo 19^3.

1. $a = 17$, $b = 6$, $p = 19$ and $i = 2$.
2. By (1), $b^2 = 36 = 17 + 1 \cdot 19$. We get $m = 1$
3. $b^{-1} \bmod 19 = 16$. By (3), $n = 9 \cdot 16 \cdot 1 \bmod 19 = 11$.
4. $x = 6 + 11 \cdot 19 \bmod 19^2 = 215$ from (2).
5. Similarly, for $b = -6 = 13$, we get $x = 146$.

A3. Find square roots of 17 modulo 19^3.

$$\begin{aligned} b^2 &= a + mp^{i-1} \bmod p^i \\ x &= b + np^{i-1} \bmod p^i \\ n &= \frac{p-1}{2} b^{-1} m \bmod p. \end{aligned}$$

Let now $i = 3$.

1. $a = 17$, $b = 215$, $p = 19$ and $i = 3$, $p^2 = 361$, $p^3 = 6859$.
2. By (1), $b^2 \equiv 5071 = 17 + 14 \cdot 361$. We get $m = 14$
3. $b^{-1} \bmod 19 = 16$. By (3), $n = 9 \cdot 16 \cdot 14 \bmod 19 = 2$.
4. $x = 215 + 2 \cdot 19^2 \bmod 19^3 = 937$ from (2).

Similarly, for $b = -215 \bmod p^2 = 146$, we get $x = -937 = 5922$.

Q4. Compute

$$2^{120} \pmod{122183}.$$

Then using the $p-1$ method, attempt to factor 122183.

A4.

- We calculate $2^{120} \bmod 122183$ by square-and-multiply as follows:

$$2^{120} = 2^{64}2^{32}2^{16}2^{8} \equiv 15068 \bmod 122183.$$

- We also know that $120 = 5! = 5 \cdot 4 \cdot 3 \cdot 2$.
- According to Pollard $p-1$, we set $a = 2^{B!} \equiv 15068 \bmod 122183$ where $B = 5$.
- Then, we calculate $d = \gcd(a-1, n) = \gcd(15067, 122183) = 61$. Since $1 < d < n$, we conclude that 61 is a factor of 122183. Indeed, we can see $122183 = 61 \cdot 2003$.
- Note this worked because all prime power divisors of $d - 1 = 60 = 2^2 \cdot 3 \cdot 5$ were less than or equal to $B = 5$.

Q5. Let $n = pq$, where p and q are primes. We can assume that $p > q > 2$ and we denote $d = \frac{p-q}{2}$ and $x = \frac{p+q}{2}$. Then $n = x^2 - d^2$. Attempt to factor $n = 400219845261001$ by searching for small non-negative integers t such that $x^2 - n = (\lceil \sqrt{n} \rceil + t)^2 - n$ is a perfect square. (This is a simple form of the Quadratic Sieve method.)

A5. The task is to search for small non-negative t such that $(\lceil\sqrt{n}\rceil + t)^2 - n$ is a perfect square, and as a result we have an equation like $n = a^2 - b^2 = (a+b)(a-b)$ with a, b known and we find the factors of n. We set $n = 400219845261001$ and try for $t = 1 \ldots$:

- $t \leftarrow 1$, $(20005496 + 1)^2 - 400219845261001 = 64956008$ is not a square.
- $t \leftarrow 2$, $(\lceil\sqrt{n}\rceil + 2)^2 - n = 104967003$ is not a square.
- $t \leftarrow 3$, $(\lceil\sqrt{n}\rceil + 3)^2 - n = 144978000$ is not a square.
- $t \leftarrow 4$, $(\lceil\sqrt{n}\rceil + 4)^2 - n = 184988999$ is not a square.
- $t \leftarrow 5$, $(20005501)^2 - n = 225000000 = 15000^2$.

We now have the factors: 20005501 ± 15000 and $400219845261001 = 19990501 \times 20020501$. This worked because p, q were too close to each other.

Q6.

1. Bob : (n, b_1), Charlie : (n, b_2), and $\gcd(b_1, b_2) = 1$
2. Alice: $y_1 = x^{b_1} \bmod n \Longrightarrow$ Bob and $y_2 = x^{b_2} \bmod n \Longrightarrow$ Charlie
3. Oscar intercepts y_1 and y_2, and performs
   i) Compute $c_1 = b_1^{-1} \bmod b_2$
   ii) Compute $c_2 = (c_1 b_1 - 1)/b_2$
   iii) Compute $x_1 = y_1^{c_1}(y_2^{c_2})^{-1} \bmod n$

1. Prove that the value x_1 computed in step iii) is in fact Alice's plaintext, x. Thus Oscar can decrypt the message Alice sent, even though the cryptosystem may be "secure".
2. Illustrate the attack by computing x by this method if $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$ and $y_2 = 14702$.

A6.

We recall the three equations from the problem description:

$$c_1 = b_1^{-1} \mod b_2 \tag{4}$$
$$c_2 = (c_1 b_1 - 1)/b_2 \tag{5}$$
$$x_1 = y_1^{c_1}(y_2^{c_2})^{-1} \mod n \tag{6}$$

1. In (4) both b_1 and b_2 are public and relatively prime thus Oscar can compute c_1.
2. In (5) note $c_1 b_1 = 1 + kb_2$ and thus $c_1 b_1 - 1$ is divisible by b_2.
3. Rearranging (5) as $b_1 c_1 - b_2 c_2 = 1$ and combining with (6) we get

$$x_1 = y_1^{c_1}(y_2^{c_2})^{-1} = x^{b_1 c_1}(x^{b_2 c_2})^{-1} = x^{b_1 c_1 - b_2 c_2} = x$$

4. x_1 is indeed the original plaintext x, which Oscar has recovered without knowledge of the private keys or factoring the modulus.

A6-b). We calculate

$$
\begin{aligned}
c_1 &= 43^{-1} \mod 7717 = 2692 \\
c_2 &= (2692 \cdot 43 - 1)/7717 = 15 \\
x_1 &= 12677^{2692} \cdot (14702^{15})^{-1} \mod 18721 \\
&= 13145 \cdot (3947)^{-1} \mod 18721 \\
&= 13145 \cdot 5668 = 15001 \mod 18721
\end{aligned}
$$

and the plaintext $x_1 = x = 15001$. We can verify this as

$$
\begin{aligned}
15001^{43} \mod 18721 = 12677 = y_1 \\
15001^{7717} \mod 18721 = 14702 = y_2
\end{aligned}
$$