T-79.5501 Cryptology Spring 2009

Homework 9

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

16th April 2009

Q1. Suppose that $n = 355044523$ is the modulus and $b = 311711321$ is the public exponent in the *RSA Cryptosystem*. Using Wiener's Algorithm, attempt to factor n. If you succeed, determine also the secret exponent a and $\phi(n)$.

A1. Set $n = 355044523$ and $b = 311711321$. We run the Euclidean algorithm as

$$\begin{aligned}
311711321 &= 0 \cdot 355044523 + 311711321 \\
355044523 &= 1 \cdot 311711321 + 43333202 \\
311711321 &= 7 \cdot 43333202 + 8378907 \\
43333202 &= 5 \cdot 8378907 + 1438667 \cdots
\end{aligned}$$

Then we build the following table:

$$c_j = q_j c_{j-1} + c_{j-2}, \quad d_j = q_j d_{j-1} + d_{j-2}$$

j	r_j	q_j	c_j	d_j	$n' = (d_j b - 1)/c_j$
0	311711321	0	1	0	—
1	355044523	0	0	1	—
2	311711321	1	1	1	311711320
3	43333202	7	7	8	356241509.57
4	8378907	5	36	41	355004560
	...				

A1. We are looking for integer solutions to

$$x^2 - (n - n' + 1)x + n = 0$$

- $j = 2$ yields no integer solutions.
- $j = 3$ has a non-integer n'.
- At $j = 4$ we get $x^2 - 39964x + 355044523 = 0$ and we have the solutions $x = 19982 \pm 6651$, namely, $p = 26633$ and $q = 13331$. Also, we get $a = d_4 = 41$ and $\phi(n) = n' = 355004560$.

Q2. Bob is using the *Rabin Cryptosystem*. Bob's modulus is $40741 = 131 \cdot 311$. Alice knows Bob's modulus but not its factors. Alice wants to remind Bob of a date in May and sends it to Bob encrypted. The ciphertext is 24270.

1. Show how Bob decrypts the ciphertext. One of the possible plaintexts is a date, which Bob accepts and discards the other decryptions.
2. Alice happens to see one of the decryptions discarded by Bob. It is 5959. Show how Alice can now factor Bob's modulus.

A2-a).

- To decrypt, Bob must calculate the four square roots of the ciphertext c modulo n.
- Applying the extended Euclidean algorithm to (p, q) Bob finds $1 = up + vq = 19 \cdot 131 - 8 \cdot 311$ from where $131^{-1} \bmod 311 = 19$ and $311^{-1} \bmod 131 = -8 \bmod 131 = 123$.
- Recall Euler's criterion that says if y is a quadratic residue modulo p, then $y^{(p-1)/2} \equiv 1 \pmod{p}$. As $p \equiv q \equiv 3 \pmod{4}$, the square roots modulo p and q are $\pm y^{(p+1)/4}$ and $\pm y^{(q+1)/4}$. Hence, we calculate

$$m_p = \sqrt{c} \mod p = c^{(p+1)/4} \mod p = 24270^{33} \mod 131 = 64$$
$$m_q = \sqrt{c} \mod q = c^{(q+1)/4} \mod q = 24270^{78} \mod 311 = 50.$$

Using CRT we get the four square roots modulo n as

$$\begin{aligned} r &= 19 \cdot 131 \cdot 50 - 8 \cdot 311 \cdot 64 \mod 40741 = 5959 \\ -r &= n - r = 34782 \\ s &= 19 \cdot 131 \cdot 50 + 8 \cdot 311 \cdot 64 \mod 40741 = 39236 \\ -s &= n - s = 1505 \end{aligned}$$

and knowing the ciphertext is a date, we recover 1505 so the date is May 15.

A2-b). Seeing Bob discard 5959, Alice now knows all square roots of c modulo n and can easily factor n by computing $\gcd(1505 + 5959, n) = 311$ and $n = 311 \cdot 131$ (Lecture 9, Slide 8).

Q3. Bob and Bart are using the Rabin Cryptosystem. Bob's modulus is 2183 and Bart's modulus is 2279. Alice wants to send an integer x, $0 < x < 2183$, encrypted to both of them. She sends ciphertext 1479 to Bob and the ciphertext 418 to Bart. Carol sees the ciphertexts and she knows Bob's and Bart's moduli. Show how Carol can compute x without factoring of moduli. Hint: Use Chinese Remainder Theorem.

A3. From the problem description, the following congruences satisfy:

$$x^2 \equiv 1479 \mod 2183$$
$$x^2 \equiv 418 \mod 2279$$

- Using the Extended Euclidean algorithm, we get $2183^{-1} \equiv 546 \bmod 2279$ and $2279^{-1} \equiv 1660 \bmod 2183$.
- Using CRT, we get

$$x^2 = 1479 \cdot 2279 \cdot 1660 + 418 \cdot 2183 \cdot 546 = 4016016 \mod 2183 \cdot 2279.$$

- Since $x < 2183$, we know $x^2 < 2183 \cdot 2279$ and it follows $x = \sqrt{4016016} = 2004$. Carol has now computed x without factoring modulii.

Q4.
It is given that

$$12^{2004} \equiv 4815 \pmod{50101},$$

where 50101 is a prime. Show that the element $\alpha = 4815$ is of order 25 in the multiplicative group $\mathbf{Z}^*_{50101}$.

A4.

- By Fermat's little theorem $\beta^{p-1} \equiv 1 \pmod{p}$.
- Given the equation $12^{2004} \equiv 4815 \pmod{50101}$ it follows

$$(12^{2004})^{25} \equiv 4815^{25} = 12^{50100} \equiv 1 \pmod{50101}.$$

  We see 4815 has multiplicative order dividing 25, so $\operatorname{ord}(4815) \in \{1, 5, 25\}$.
- Obviously, the $\operatorname{ord}(4815)$ cannot be 1 since $4815^1 \neq 1 \bmod 50101$. Also, it cannot be 5 since $4815^5 = 46880 \neq 1 \bmod 50101$. It follows that the order of 4815 is 25.

Q5.
Consider $p = 1231$, which is a prime. Find an element of order $q = 41$ in the multiplicative group $\mathbf{Z}_{1231}^*$.

A5. Let us choose any element $\alpha \in \mathbf{Z}_p^*$ such that $\alpha^{(p-1)/41} \neq 1 \pmod{p}$. Let $\beta = \alpha^{(p-1)/41} \neq 1 \pmod{p}$. Then, $\mathrm{ord}(\beta) > 1$ and $\beta^{41} = \alpha^{p-1} \equiv 1 \pmod{p}$. Hence, $\mathrm{ord}(\beta) \mid 41$ and since 41 is a prime we must have $\mathrm{ord}(\beta) = 41$. For example, if $\alpha = 3$, then $\beta = 3^{(p-1)/41} = 1000 \neq 1 \pmod{p}$ has order 41.

Q6.

A prime p is said to be a *safe prime* if $(p-1)/2$ is a prime.

a) Let p be a safe prime, that is, $p = 2q + 1$ where q is a prime. Prove that an element in $\mathbf{Z}_p$ has multiplicative order q if and only if it is a quadratic residue and not equal to 1 mod p.

b) The integer 08012003 is a safe prime, since 4006001 is a prime. Find some element of multiplicative order 4006001 in $\mathbf{Z}_{8012003}$.

A6.
($\Rightarrow$) Assume that $w \in \mathbf{Z}_p$ has multiplicative order q. Then $w^q \equiv 1 \bmod p$. Since $q = (p-1)/2$ it follows from Euler's criterion that w is a quadratic residue modulo p.
($\Leftarrow$) Assume that $w \neq 1$ is a quadratic residue modulo p. Then using Euler's criterion, we have $w^{(p-1)/2} = w^q \equiv 1 \bmod p$. It follows that the order of w divides q. Since q is prime, the order of w must be q (Note that w is not 1).

A6.
By a), we find some quadratic residue in $\mathbf{Z}_{8012003}$. For example, using Yacobi symbol, we get

$$\begin{aligned}
\left(\frac{2}{8012003}\right) &= -1 \Rightarrow \mathrm{ord}(2) \neq 4006001 \\
\left(\frac{3}{8012003}\right) &= -\left(\frac{2}{3}\right) = 1 \Rightarrow \mathrm{ord}(3) = 4006001 \\
\left(\frac{4}{8012003}\right) &= -\left(\frac{2}{8012003}\right) = 1 \Rightarrow \mathrm{ord}(4) = 4006001 \\
&\vdots
\end{aligned}$$