Solution Sheet 5

Cryptography and Security 2022

Solution 1 RSA with a counter

1. Confidentiality from RSA and Integrity from $\mathsf{format}(m)$.
2. Alice sends m:

$$a = x^3 \mod (N_B) \xrightarrow{\quad a \quad}$$
$$\xleftarrow{\quad repeat \quad}$$
$$b = y^3 \mod (N_B) \xrightarrow{\quad b \quad}$$

   (a) $a = (\mathsf{format}(m) \cdot 2^{32} + i)^e \bmod N_B$
   $b = (\mathsf{format}(m) \cdot 2^{32} + i + 1)^e \bmod N_B$
   Thus $y = x + 1$

   (b)

$$\begin{aligned} z^3 - a = z^3 - x^3 &= (z-x)(z^2+zx+x^2) = (z-x)\cdot\delta \qquad (1)\\ (z+1)^3 - b = (z+1)^3 - (x+1)^3 &= z^3+3z^2+3z+1-(x^3+3x^2+3x+1)\\ &= (z^3-x^3)+3(z^2-x^2)+3(z-x)\\ &= (z-x)\cdot[(z^2+zx+x^2)+3(z+x)+3]\\ &= (z-x)\cdot\gamma \qquad (2)\end{aligned}$$

   (c) As γ is prime with δ, $z - x$ is the gcd of $z^3 - a$ and $(z+1)^3 - b$ in this ring.

   (d) Compute $gcd(z^3 - a,\ (z+1)^3 - b)$ and obtain $(z - x)$. Then deduce x.

$$\begin{aligned} [(z+1)^3-b]-[z^3-a] &= 3z^2+3z+1-b+a\\ (\frac{1}{3}-\frac{z}{3})\cdot[(z+1)^3-b]+(\frac{2}{3}+\frac{z}{3})\cdot[z^3-a] &= \frac{(2-a+b)}{3}z+\frac{(1-2a-b)}{3}\\ &= \frac{2-a+b}{3}\left[z+\frac{1-2a-b}{2-a+b}\right]\\ &= \frac{2-a+b}{3}\cdot(z-x)\end{aligned} \qquad (3)$$

   $\Rightarrow x = \frac{2a+b-1}{2-a+b}$.

3. No, the order of the polynoms is to big.

Solution 2 Quadratic Residues

1. We find the QR's of $\mathbf{Z}_{35}^*$ using Table 1 which contains the square of all elements in $\mathbf{Z}_{35}^*$.

Table 1: Squares in $\mathbf{Z}_{35}^*$

$1^2 = 1$	$2^2 = 4$	$3^2 = 9$	$4^2 = 16$
$6^2 = 1$	$8^2 = 29$	$9^2 = 11$	$11^2 = 16$
$12^2 = 4$	$13^2 = 29$	$16^2 = 11$	$17^2 = 9$
$18^2 = 9$	$19^2 = 11$	$22^2 = 29$	$23^2 = 4$
$24^2 = 16$	$26^2 = 11$	$27^2 = 29$	$29^2 = 1$
$31^2 = 16$	$32^2 = 9$	$33^2 = 4$	$34^2 = 1$

Hence, by looking at the values of Table 1, we obtain the set QR_{35} of all QR's modulo 35

$$\mathrm{QR}_{35} = \{1, 4, 9, 11, 16, 29\}.$$

Then, the set QNR_{35} of the non-quadratic residues is

$$\mathrm{QNR}_{35} = \{2, 3, 6, 8, 12, 13, 17, 18, 19, 22, 23, 24, 26, 27, 31, 32, 33, 34\}.$$

We observe that every QR has four square roots.

2. By definition, the "CRT-transform" of an element $a \in \mathbf{Z}_n^*$ with respect to $p_1, \ldots, p_k$ is $(a \bmod p_1, \ldots, a \bmod p_k)$. We have to show that

$$a \in \mathrm{QR}_n \iff a \bmod p_i \in \mathrm{QR}_{p_i} \text{ for } 1 \leq i \leq k.$$

By definition, there exists an $x \in \mathbf{Z}_n^*$ such that $a = x^2 \bmod n$. Then, $a \bmod p_i = x^2 \bmod p_i$ is trivially a QR in $\mathbf{Z}_{p_i}$ for any $1 \leq i \leq k$. Conversely, one can write by assumption the "CRT-transform" of the element a as $(x_1^2, x_2^2, \ldots, x_k^2) \in \mathbf{Z}_{p_1}^* \times \cdots \times \mathbf{Z}_{p_k}^*$. Since the "CRT-transform" is a ring isomorphism, we deduce that a is the square of an element x having $(x_1, \ldots, x_k)$ as image under the "CRT-transform". Hence, $a = x^2 \bmod n$ is in QR_n.

3. From the previous question, we know that a quadratic residue $a \in \mathbf{Z}_n^*$ has an image of the form $(x_1^2, x_2^2, \ldots, x_k^2)$ under the "CRT-transform". Since $\mathbf{Z}_{p_i}$ is a field, x_i^2 has exactly 2 square roots in $\mathbf{Z}_{p_i}$ for $1 \leq i \leq k$, namely $\pm x_i$. Therefore, we have 2^k square roots in total since we have two square roots for each "CRT-component".

4. By definition of a subgroup, it suffices to show that $ab^{-1} \in \mathrm{QR}_n$ whenever a,$b \in \mathrm{QR}_n$. There exist two elements $x, y \in \mathbf{Z}_n^*$ satisfying $a = x^2$ and $b = y^2$. From this, we have $ab^{-1} = x^2 \cdot (y^2)^{-1} = (xy^{-1})^2$, which concludes the proof.

   As every element of QR_n has 2^k square roots, the order of QR_n is equal to $\varphi(n)/2^k$.

5. Let $a, b \in \mathbf{Z}_n^*$, with $a \in \mathrm{QR}_n$ and $b \in \mathrm{QNR}_n$. From Question 2, we know that there exists an integer $1 \leq j \leq k$ such that $b_j = b \bmod p_j$ is in QNR_{p_j}. Hence,

$$b^{\frac{p_j - 1}{2}} \not\equiv 1 \pmod{p_j}.$$

   As

$$a^{\frac{p_j - 1}{2}} \equiv 1 \pmod{p_j},$$

   we have

$$(ab)^{\frac{p_j - 1}{2}} \not\equiv 1 \pmod{p_j},$$

   which means that ab is not a QR modulo n.

6. Consider the elements $2, 3 \in \mathrm{QNR}_{35}$. The element $6 = 2 \cdot 3 \bmod 35$ lies in QNR_{35}. In the contrary, if we take $2, 18 \in \mathrm{QNR}_{35}$, we observe that $2 \cdot 18 \equiv 1 \pmod{35}$.

Solution 3 Modulo 101 Computation

Through *all* this exercise, we will let $p = 101$.

1. Show that p is a prime number.

   p is not divisible by any prime less than $\sqrt{p}$: 2, 3, 5, 7.

2. What is the order of $\mathbf{Z}_p^*$?

   Since p is prime, $\#\mathbf{Z}_p^* = \varphi(p) = p - 1$.

3. If $x = \sum_{i=0}^{2\ell-1} d_i 10^i$ with $0 \leq d_i < 10$ for all i, show that

$$x \equiv \sum_{i=0}^{\ell-1} (-1)^i (d_{2i} + 10 d_{2i+1}) \pmod{101}$$

   Deduce an algorithm to compute x mod 101 easily.

   We have $x = \sum_{i=0}^{\ell-1} (d_{2i} + 10 d_{2i+1}) 100^i$ Since $100 \equiv -1 \pmod{101}$ we obtain the result. To reduce modulo 101, we simply take the decimal expansion, group digits by pair and apply the above formula iteratively until the result is less than 100 in absolute value. Then, if negative we add 101 and we are done.

4. Show that every element of $\mathbf{Z}_p^*$ has a unique 7th root and give an explicit formula to compute it (recall that $p = 101$).
   Application: Find the 7th root of 2 in $\mathbf{Z}_p^*$.

   7 is invertible modulo $p - 1$. Its inverse is 43 since $7 \times 43 = 301$ which is 1 modulo 100. So, the unique 7th root of x is x^{43} mod p.

   We compute 2^{43} mod 101 using the square and multiply algorithm. We have

$$\begin{aligned} 2^{43} &\equiv 2^{1+2\cdot(1+2^2\cdot(1+2^2))} \\ &\equiv 2 \times 4^{1+2^2\cdot(1+2^2)} \\ &\equiv 2 \times 4 \times 54^{1+2^2} \\ &\equiv 2 \times 4 \times 54 \times (-13)^2 \\ &\equiv 2 \times 4 \times 54 \times 68 \\ &\equiv 86 \end{aligned}$$

   We can check that $86^7 \equiv 2$.

5. Given $g \in \mathbf{Z}_p^*$ we let $y = g^{10} \bmod p$. Using 3 multiplications modulo p and 2 tests, give an algorithm with input y to decide whether g is a generator or not (recall that $p = 101$).
   Application: show that 2 is a generator.

   Since $p-1 = 2^2 \times 5^2$, g is a generator iff $g^{\frac{p-1}{2}} \bmod p \neq 1$ and $g^{\frac{p-1}{5}} \bmod p \neq 1$. We have $g^{\frac{p-1}{2}} \equiv y^5$ and $g^{\frac{p-1}{5}} \equiv y^2$. So, we compute $a \equiv y^2$, $b \equiv a^2$, $c \equiv yb$ and we check that $a \not\equiv 1$ and $c \not\equiv 1$.

   For $g = 2$, we compute

$$\begin{aligned} 2^{10} &\equiv 2^{2\cdot(1+2^2)} \\ &\equiv 4^{1+2^2} \\ &\equiv 4 \times 4^{2^2} \\ &\equiv 4 \times 16^2 \\ &\equiv 4 \times 54 \\ &\equiv 14 \end{aligned}$$

   so $y = 14$. We now compute $a = 95$, $b = 36$, and $c = 100$. Since neither a nor c is 1, 2 is a generator.

6. Under which condition is x a quadratic residue in $\mathbf{Z}_p^*$?

   It is equivalent to $x^{\frac{p-1}{2}} \bmod p = 1$.

7. Show that 5 is a quadratic residue in $\mathbf{Z}_p^*$.

   We have

$$\begin{aligned} 5^{50} &\equiv 5^{2\cdot(1+2^3\times(1+2))} \\ &\equiv 25^{1+2^3\times(1+2)} \\ &\equiv 25 \times 25^{2^3\times(1+2)} \\ &\equiv 25 \times 19^{2^2\times(1+2)} \\ &\equiv 25 \times 58^{2\times(1+2)} \\ &\equiv 25 \times 31^{1+2} \\ &\equiv 25 \times 31 \times 31^2 \\ &\equiv 25 \times 31 \times 52 \\ &\equiv 1 \end{aligned}$$

   so 5 is a quadratic residue.

8. Show that 10 is a 4th root of 1 in $\mathbf{Z}_p^*$.

   We have $10^2 = 100 \equiv -1$ so $10^4 \equiv 1$.

9. Show that for all $y \in \mathbf{Z}_p^*$ we have that $y^{\frac{p-1}{4}}$ is 10^k for some $k \in \{0, 1, 2, 3\}$.

   Since $\mathbf{Z}_p$ is a field, there are no more than 4 4th roots of 1 and these are all powers of 10: 1, 10, 100, and 91. Since $\left(y^{\frac{p-1}{4}}\right)^4 \equiv y^{p-1} \equiv 1$ in $\mathbf{Z}_p^*$, then $y^{\frac{p-1}{4}}$ must be one of these 4th roots of 1.

   Show that $y^{\frac{p+3}{4}}$ can be written $y \times 10^k$.

   We have $y^{\frac{p+3}{4}} = y \times y^{\frac{p-1}{4}} = y \times 10^k$.

10. Deduce that if x is a quadratic residue then either $x^{\frac{p+3}{8}}$ or $10x^{\frac{p+3}{8}}$ is a square root of x. Provide an algorithm to extract square roots in $\mathbf{Z}_p^*$.

    If $x \equiv y^2$ then $x^{\frac{p+3}{8}} \equiv y^{\frac{p+3}{4}} \equiv y \times 10^k$ so its square is $x \times (-1)^k$. If k is even then this is a square root of x. If not, we multiply it by 10 and the power of 10 becomes even.

    To compute square roots of quadratic residues, we just raise to the power $\frac{p+3}{8} = 13$ and we multiply by 10 if it is not a square root.

11. Find a square root of 5.

    We have

$$\begin{aligned} 5^{13} &\equiv 5^{1+2^2\times(1+2)} \\ &\equiv 5 \times 5^{2^2\times(1+2)} \\ &\equiv 5 \times 25^{2\times(1+2)} \\ &\equiv 5 \times 19^{1+2} \\ &\equiv 5 \times 19 \times 19^2 \\ &\equiv 5 \times 19 \times 58 \\ &\equiv 56 \end{aligned}$$

    which is a square root of 5.