*Cryptography and Security 2016*

# Solution Sheet 5

## Solution 1 Authenticated Diffie-Hellman Key Agreement Protocol

1. $A$ knows its secret key $X_A$, the public keys $Y_A = g^{X_A} \bmod p$, $Y_B = g^{X_B} \bmod p$, ephemeral secret key $a$ and ephemeral public keys $v = g^a \bmod p$, $w = g^b \bmod p$. So, it can compute as follows:

$$K = Y_B^a w^{X_A} \mod p$$

2. $A^*$ starts the protocol as it is $A$. It picks $a \in \mathbb{Z}_q$ and sends $g^a \mod p$ to $B$. When it receives $w$ from $B$, $A^*$ tries to find $b$ as follows: It picks a number $b'$ from the set which includes these small numbers, until finding $b'$ such that $g^{b'} = w$. Remark that $b$ can be efficiently found with this algorithm because the set is small (e.g., for length of around 40 bits , at most $2^{40}$ iterations is enough to find $b$).

   After finding $b$, it computes $K = Y_B^a Y_A^b$.

   To prevent this attack, $B$ should use unbiased pseudorandom generator.

3. $A^*$ starts the protocol as it is $A$. It picks $a \in \mathbb{Z}_q$ and sends $v = g^a \mod p$ to $B$. When it receives $w = g^b \bmod p = g^{ac} \bmod p$ from $B$, $A^*$ tries to find $c$ as follows: Assume that $c \in N = \{1, ..., n\}$ where $n$ is a small number. It iteratively picks a number $c' \in N$ until finding $c'$ such that $v^{c'} = w$. Since $n$ is small, this algorithm is efficient.

   After finding $c$, it computes $K = Y_B^a Y_A^{ca}$.

   To prevent this attack, $B$ should pick $b$ randomly from $\mathbb{Z}_q$.

## Solution 2 Square Roots

1. 1: **repeat**
   2: Pick a random $y_0 \in \{1, \ldots, n-1\}$.
   3: compute $x \coloneqq y_0^2 \bmod n$.
   4: Get $y \leftarrow \mathcal{O}(x)$.
   5: **until** $y \neq y_0$ and $y \neq -y_0 \bmod n$
   6: **return** $\gcd(y - y_0, n)$ which is one of the factors.

2. There are two square roots $\pm y_p$ of $x$ mod $p$ and two square roots $\pm y_q$ of $x$ mod $q$. The four square roots of $x$ mod $n$ correspond to $\mathrm{CRT}(\pm y_p, \pm y_q)$ for all sign combinations.

   If $y \neq y_0$ and $y \neq -y_0$, this means that $y$ and $y_0$ have a different square root mod $p$ or mod $q$ (it's an exclusive or). Let's say wlog that they differ mod $p$. Then, $y \neq y_0 \bmod p$ and $y = y_0 \bmod q$. Hence, $y - y_0 \neq 0 \bmod p$ and $y - y_0 = 0 \bmod q$. We have, thus, that $y - y_0$ is a factor of $q$ and not of $p$ and we get $q$ through the gcd.

3. There are four square roots mod $n$ and only two of them gives us a factor (the other two are either $y_0$ or $-y_0$). Hence, we need two queries in average. The complexity of the algorithm is $O((\log(n))^2 + |\mathrm{SQRT}|)$, where $|\mathrm{SQRT}|$ is the complexity of the oracle.

## 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.