Solution Sheet #5

Advanced Cryptography 2021

Solution 1 Perfect Unbounded IND is Equivalent to Perfect Secrecy

1. First note that in any case, for any x and y we have

   $$\Pr[Y = y, X = x] = \Pr[C_K(X) = y, X = x] = \Pr[C_K(x) = y, X = x] = \Pr[C_K(x) = y]\Pr[X = x]$$

   If C provides perfect secrecy, then, we deduce $\Pr[Y = y, X = x] = \frac{1}{\#\mathcal{M}}\Pr[X = x]$. By summing this over x, we further obtain $\Pr[Y = y] = \frac{1}{\#\mathcal{M}}$. So, $\Pr[Y = y, X = x] = \Pr[Y = y]\Pr[X = x]$ for all x and y: X and Y are independent.

   Conversely, if X and Y are independent, the above property gives

   $$\Pr[C_K(X) = y]\Pr[X = x] = \Pr[Y = y]\Pr[X = x] = \Pr[Y = y, X = x] = \Pr[C_K(x) = y]\Pr[X = x]$$

   Since X has support $\mathcal{M}$, we have $\Pr[X = x] \neq 0$, so we can simplify by $\Pr[X = x]$ and get $\Pr[C_K(X) = y] = \Pr[C_K(x) = y]$ for all x and y. This implies that $\Pr[C_K^{-1}(y) = x]$ does not depend on x, so $C_K^{-1}(y)$ is uniformly distributed, for all y. So, $\Pr[C_K(x) = y] = \frac{1}{\#\mathcal{M}}$ for all x and y. Therefore, $C_K(x)$ is uniformly distributed for all x: C provides perfect secrecy as defined in this exercise.

2. Since we have perfect secrecy, when b and r are fixed and k random, y is uniformly distributed whatever b. So, the distribution of $b' = \mathcal{A}(y; r)$ does not depend on b when b and r are fixed. So, $\Pr_k[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_k[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$ for all r. Thus, on average over r, we have $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_{r,k}[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$. Therefore, we have perfect unbounded IND-security.

3. We define the following adversary $\mathcal{A}$. First, $\mathcal{A}(; r)$ produces $m_0 = x_1$ and $m_1 = x_2$. Then, $\mathcal{A}(y; r) = 1$ if and only if $y = z$.

   We have $\Pr_k[\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A}) = 1] = \Pr[C_K(x_b) = z]$. Furthermore, since $\mathcal{A}$ is deterministic, $\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A})$ does not depend on r. So, $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A}) = 1] = \Pr[C_K(x_b) = z]$.

   Since the cipher is perfect unbounded IND-secure, we have $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_{r,k}[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$. Therefore, $\Pr[C_K(x_1) = z] = \Pr[C_K(x_2) = z]$.

   We deduce that the distribution of $C_K(x)$ does not depend on x.

4. Given x_0 and y, we have that

   $$\Pr[C_K(x_0) = y] \times \#\mathcal{M} = \sum_x \Pr[C_K(x) = y] = \sum_x \Pr[C_K^{-1}(y) = x] = 1$$

   The first equality comes from the previous question. So, $\Pr[C_K(x_0) = y] = 1/\#\mathcal{M}$: $C_K(x_0)$ is uniformly distributed, for any x_0. Therefore, we have perfect secrecy.

Solution 2 ElGamal using a Strong Prime

1. Let h be a generator of $\mathbf{Z}_p^*$. Clearly, h^2 has order q. It further generates only quadratic residues. So, $g = h^2$ is a generator of QR_p.

2. We have $\left(\frac{(-1)}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^q = -1$ since q is large and prime. So, the Legendre symbol of -1 is -1. We deduce that -1 is not a quadratic residue modulo p.

3. Actually, $((-x)/p) = ((-1)/p).(x/p) = -(x/p)$. So, $-x$ and $+x$ have opposite Legendre symbols. Since $x \in \mathbf{Z}_p^*$, this is not 0. So, either $-x$ or $+x$ has a Legendre symbol equal to $+1$ but not both. This is the unique quadratic residue $\sigma(x)$.

   Clearly, the sets $\{-x, +x\}$ are disjoint for all $x = 1, \ldots, q$. So, the mapping is injective. Now, since half of the elements in $\mathbf{Z}_p^*$ are in QR_p, we have exactly q of them. So, the sets $\{1, \ldots, q\}$ and QR_p have the same cardinality. Therefore, σ is a bijection.

4. If $m^q \bmod p = 1$, we set $\sigma(m) = m$, otherwise $\sigma(m) = -m$.

   If $x \bmod p \leq q$, we set $\sigma^{-1}(x) = x \bmod p$, otherwise $x = p - (x \bmod p)$.

5. To decrypt (u, v), we compute $\sigma^{-1}(vu^{-x} \bmod p)$. Here, $\sigma^{-1}(x)$ is the only value between $x \bmod p$ and $(-x) \bmod p$ which is lower or equal to q.

Solution 3 Pohlig-Hellman

First, notice that g is a generator of $\mathbb{Z}_{13}$ and, hence, has order 12. The factorization of 12 is $2^2 \times 3$. Let x be the wanted discrete logarithm. We are first looking for $x \bmod 3$. We have $g^{n/3} = 6^{12/3} = 6^4 = 9$ and $y^{n/3} = 3$. Hence, the discrete logarithm of 3 in basis 9 is 2 and we get that $x \bmod 3 = 2$.

Now we recover $x \bmod 4$. To do this, we will first need to recover $u_0 := x \bmod 2$. We have $g'' = g^{n/2} = 6^{12/2} = 6^6 = 12$ and $y'' = y^{n/2} = 12$. Hence, the discrete logarithm of 12 in basis 12 is 1. Thus, $u_0 = x \bmod 2 = 1$. This will be the least significant bit of $x \bmod 4$. To recover the second bit u_1, we compute $y' = y^{12/4}/g^{12u_0/4} = 5/8 = 12$. Hence, we need to compute the discrete logarithm of $y'' = 12^{2^0} = 12$ in basis $g'' = 12$ which is 1. Thus, $u_1 = 1$ and we get $x \bmod 4 = u_1 \times 2 + u_0 = 1 \times 2 + 1 = 3$.

Wrapping up, we have $x \bmod 3 = 2$ and $x \bmod 4 = 3$. Hence, by the Chinese remainder theorem, $x = 11 \bmod 12$.