Exercise Sheet #5

Advanced Cryptography 2021

Exercise 1 Perfect Unbounded IND is Equivalent to Perfect Secrecy (Final 2012)

Given a message block space $\mathcal{M}$ and a key space $\mathcal{K}$, we define a *block cipher* as a deterministic algorithm mapping (k, x) for $k \in \mathcal{K}$ and $x \in \mathcal{M}$ to some $y \in \mathcal{M}$. We denote $y = C_k(x)$. The algorithm must be such that there exists another algorithm C_k^{-1} such that for all k and x, we have $C_k^{-1}(C_k(x)) = x$.

We say that C provides *perfect secrecy* if for each x, the random variable $C_K(x)$ is uniformly distributed in $\mathcal{M}$ when the random variable K is uniformly distributed in $\mathcal{K}$.

Given a bit b, we define the following game.

Game $\mathsf{IND}(b)$:
1: pick random coins r
2: pick $k \in \mathcal{K}$ uniformly
3: run $(m_0, m_1) \leftarrow \mathcal{A}(;r)$
4: compute $y = C_k(m_b)$
5: run $b' \leftarrow \mathcal{A}(y; r)$

Given some fixed b, r, k, the game is deterministic and we define $\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A})$ as the outcome b'. We say that C provides *perfect unbounded IND-security* if for any (unbounded) adversary $\mathcal{A}$ playing the above game, we have $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_{r,k}[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$. (That is, the probability that $b' = 1$ does not depend on b.)

1. This question is to see the link with a more standard notion of perfect secrecy.

   Let X be a random variable of support $\mathcal{M}$, let K be independent, and uniformly distributed in $\mathcal{K}$, and let $Y = C_K(X)$. Show that X and Y are independent if and only if C provides perfect secrecy as defined in this exercise.

   Hint: first show that for all x and y, $\Pr[Y = y, X = x] = \Pr[C_K(x) = y] \Pr[X = x]$. Then, deduce that if C provides perfect secrecy, then Y is uniformly distributed which implies that X and Y are independent. Conversely, if X and Y are independent, deduce that for all x and y we have $\Pr[C_K(X) = y] = \Pr[C_K(x) = y]$. Deduce that $C_K^{-1}(y)$ is uniformly distributed then that $C_K(x)$ is uniformly distributed.

2. Show that if C provides perfect secrecy, then it is perfect unbounded IND-secure.

3. Show that if C is perfect unbounded IND-secure, then for all $x_1, x_2, z \in \mathcal{M}$, we have that $\Pr[C_K(x_1) = z] = \Pr[C_K(x_2) = z]$ when K is uniformly distributed in $\mathcal{K}$.

   Hint: define a deterministic adversary $\mathcal{A}_{x_1,x_2,z}$ based on x_1, x_2, and z.

4. Deduce that if C is perfect unbounded IND-secure, then it provides perfect secrecy.

Exercise 2 ElGamal using a Strong Prime (Final 2013)

Let p be a large strong prime. I.e., p is a prime number and $q = \frac{p-1}{2}$ is prime as well.

1. Show that QR_p is a cyclic group.
2. Show that -1 is not a quadratic residue modulo p.
3. Show that there exists a bijection σ from $\{1, \ldots, q\}$ to QR_p, the group of quadratic residues in Z_p^*, such that for all x, $\sigma(x) = x$ or $\sigma(x) = -x$.
4. For $m \in \{1, \ldots, q\}$ and $x \in \mathsf{QR}_p$, give algorithms to compute $\sigma(m)$ and $\sigma^{-1}(x)$.
5. We consider the following variant of the ElGamal cryptosystem over the message space $\{1, \ldots, q\}$. Let g be a generator of QR_p. The secret key is $x \in \mathbf{Z}_{p-1}$. The public key is $y = g^x \bmod p$. To encrypt a message m, we pick $r \in \mathbf{Z}_{p-1}$, compute $u = g^r \bmod p$, and $v = \sigma(m)y^r \bmod p$. The ciphertext is the pair (u, v).

   Describe the decryption algorithm.

Exercise 3 Pohlig-Hellman

I think you'll see Pohlig-Hellman next week, so it's probably best if you try this exercise then. Compute the discrete logarithm of $y = 11$ in basis $g = 6$ in $\mathbb{Z}_{13}^*$ using the Pohlig-Hellman algorithm.

Hint:

$$y^3 \bmod 13 = 5; y^6 \bmod 13 = 12; y^4 \bmod 13 = 3$$
$$g^3 \bmod 13 = 8; g^6 \bmod 13 = 12; g^4 \bmod 13 = 9$$