Crypto & Codes MAMME Fall 2013
Exercises:
Cryptography (part 1/2)

Reductions

1. Write a reduction showing that the Computational Diffie-Hellman (CDH) problem in a cyclic group $G = \langle g \rangle$ of known order q can be reduced to the Square in the Exponent (SE) problem in the same group. SE problem is, given (g, g^x), for a random $x \in \mathbb{Z}_q$, to compute g^{x^2}. Is the reduction tight?

   Hint: use the equality $xy = \frac{1}{2}((x+y)^2 - x^2 - y^2)$

2. Do the same for the Cube in the Exponent problem, that is, given (g, g^x), for a random $x \in \mathbb{Z}_q$, to compute g^{x^3}.

   Hint: use the previous exercise and simply reduce SE problem to the Cube in the Exponent problem.

3. Find a reduction of the Composite Residuosity (CR) problem, that is, given $n = pq$ and $(1+mn)r^n \mod n^2$ for random $m \in \mathbb{Z}_n$ and $r \in \mathbb{Z}_{n^2}^\times$ find m, to the $RSA(n, n)$ problem. In general, the $RSA(n, e)$ problem for $n = pq$ and e coprime with $(p-1)(q-1)$ is, given (n, e, x^e) for a random $x \in \mathbb{Z}_n^\times$, to compute x.

4. Show that the permutation $T(A, B, C) = (C, A, B)$ transforms an instance of the Decision Inverse in the Exponent (DIE) problem into an instance of the Decision Square in the Exponent (DSE) problem, preserving the probability distributions for 'YES' and 'NO' instances (also called 'Real' and 'Random' instances). An instance of DIE problem in a cyclic group G of known order q is the tuple (g, g^x, g^r), where g is a random generator of G, x is a random element in $\mathbb{Z}_q^\times$ and $r = x^{-1} \mod q$ for a 'YES' instance, while r is a random element in $\mathbb{Z}_q^\times$ for a 'NO' instance. Instances of the DSE problem are defined in the same way but now $r = x^2 \mod q$ for a 'YES' instance.

   Hint: observe that here g is a random generator. Therefore g_{DIE} can be different from g_{DSE}.

One-Way Functions

1. Consider two function families $\mathcal{F} = \{f_k : X_k \to Y_k\}_{k\in\mathcal{K}}$ and $\mathcal{G} = \{g_k : Y_k \to Z_k\}_{k\in\mathcal{K}}$, and their composition $\mathcal{H} = \{g_k \circ f_k : X_k \to Z_k\}_{k\in\mathcal{K}}$. Show that

   (a) If $\mathcal{F}$ is uniform (i.e., if x is uniformly distributed on X_k then so is $f_k(x_k)$ on Y_k) and $\mathcal{G}$ is one-way then $\mathcal{H}$ is one-way. **Hint:** prove the contrapositive implication by showing a reduction.

   (b) If $\mathcal{F}$ is one-way and $\mathcal{G}$ is injective then $\mathcal{H}$ is one-way.

   (c) If $\mathcal{H}$ is one-way then $\mathcal{F}$ or $\mathcal{G}$ are one-way.

   (d) What happens if $\mathcal{F}$ is one-way but $\mathcal{G}$ is not injective. **Hint:** use the fact that a constant function cannot be one-way. (Why?)

   (e) What happens if $\mathcal{G}$ is one-way but $\mathcal{F}$ is not uniform (e.g., it is not even surjective). Give an example.

2. Consider two function families $\mathcal{F} = \{f_k : X_k \to Y_k\}_{k\in\mathcal{K}}$ and $\mathcal{G} = \{g_k : X_k \to Z_k\}_{k\in\mathcal{K}}$, and define $\mathcal{H} = \{h_k : X_k \to Y_k \times Z_k\}_{k\in\mathcal{K}}$ such that $h_k(x) = (f_k(x), g_k(x))$. Show that if $\mathcal{H}$ is one-way then $\mathcal{F}$ and $\mathcal{G}$ are one-way.

3. Consider two function families $\mathcal{F} = \{f_k : X_k \to Z_k\}_{k\in\mathcal{K}}$ and $\mathcal{G} = \{g_k : Y_k \to T_k\}_{k\in\mathcal{K}}$, and define $\mathcal{H} = \{h_k : X_k \times Y_k \to Z_k \times T_k\}_{k\in\mathcal{K}}$ such that $h_k(x, y) = (f_k(x), g_k(y))$. Show that if $\mathcal{H}$ is one-way then $\mathcal{F}$ or $\mathcal{G}$ are one-way.

4. Show that any family of uniform functions $\mathcal{F} = \{f_k : W_k \to L_k\}_{k\in\mathcal{K}}$ for a hard membership problem $L_k \subset X_k$ has to be a one-way function family. Assume that one can efficiently verify whether or not an arbitrary string encodes an element in W_k.

   Hint: show a reduction that uses any algorithm inverting $\mathcal{F}$ to tell apart elements uniformly distributed in L_k from elements uniformly distributed in $X_k \setminus L_k$.

Symmetric Key Cryptography

1. Try to extend the one-time pad to the integers, by relaxing the notion of perfect symmetric encryption. Instead of showing that for a random key $k \in K_\ell$ and a random message $m \in M_\ell$, the message m and its encryption c are independent random variables, assume that the statistical distance between (m, c) and a uniform distribution on $M_k \times C_k$ is smaller that ϵ, for a suitable ϵ (e.g., a negligible function in ℓ). Recall that the statistical distance between two random variables X, Y defined on a set $\mathcal{T}$ is defined by

$$\mathrm{dist}(X, Y) = \frac{1}{2}\sum_{t\in\mathcal{T}} |\Pr[X = t] - \Pr[Y = t]|$$

(a) Show that the statistical distance between the uniform distributions on $\mathcal{T}$ and on a subset $\mathcal{T}'$ of $\mathcal{T}$ equals $1 - \frac{|\mathcal{T}'|}{|\mathcal{T}|}$

(b) Define $M_\ell = \{0, \ldots, 2^\ell - 1\}$, $K_\ell = \{0, \ldots, 2^\tau - 1\}$ and $C_\ell = \{0, \ldots, 2^\ell + 2^\tau - 2\}$, for some τ related to the parameter ℓ, and define the encryption function of $m \in M_\ell$ as $c = m + k$. Then show that (m, c) is uniformly distributed on a subset of $M_\ell \times K_\ell$ of size $2^{\ell+\tau}$. As a consequence, show that the encryption scheme has ϵ one-time security for $\epsilon = 2^{-(\tau-\ell)}$.

2. What is the minimal size of the key in a perfectly secure n-times symmetric encryption scheme, compared to the size of the message?

3. Show that CBC mode of operation cannot handle arbitrarily long messages. Recall that CBC mode is described by the equations $c_0 = iv,\ c_i = \mathsf{Enc}(k, m_1 \oplus c_{i-1})$.

(a) What can be learnt by an adversary from the event that two ciphertext blocks are equal (say, $c_i = c_{i+r}$, for some $i > 0$ and some $r > 0$)? Is this enough to break IND security?

(b) How many blocks (or what length of the plaintext) makes the previous considerations a successful attack? Assume that ciphertext blocks behave like independent random variables, and also assume that the probability of finding two equal blocks among n randomly chosen can be approximated (birthday paradox) by $\frac{n^2}{2N}$, where N is the cardinality of the ciphertext space of the block cipher.

(c) If a success probability of 2^{-20} starts to be considered as dangerous, what is the maximum recommended length for the plaintext (in Megabytes) for ciphertext block lengths of 32, 64 and 128 bits?

4. Show that $MAC((k_0, k_1, \ldots, k_n), (m_1, \ldots, m_n)) = k_0 + k_1 m_1 + \ldots + k_n m_n \mod q$ for a prime q and $k_i \in \mathbb{Z}_q$, $m_j \in \mathbb{Z}_q$ defines a perfect one-time message authentication code with message space $\mathbb{Z}_q^n$, key space $\mathbb{Z}_q^{n+1}$ and tag space $\mathbb{Z}_q$.

Hint: just prove that the MAC is defined from a pairwise independent hash family.

Public Key Encryption

1. From the homomorphic properties of ElGamal public key encryption scheme, show several possible attacks breaking the IND-CCA security.

2. Do the same with Paillier's encryption scheme.

3. Extend the impossibility result that deterministic encryption cannot achieve IND-CPA security, to probabilistic encryption with low randomness.

(a) Show a generic attack breaking IND-CPA security with probability at least $1/\min_{m \in M} |C_m|$, where C_m is the set of all possible encryptions of a message $m \in M$, that runs in constant time (i.e., the attack takes no longer than a constant number of encryptions).

(b) Now show an attack that succeeds with overwhelming probability (one minus a negligible function), perhaps with a nonconstant expected running time.

4. Use any successful adversary against the OW-CPA security of a public key encryption scheme to break the IND-CPA security.