EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Endsem Exam : 45 points May 3, 2018

1. (a) (2 points) Define perfectly secret encryption schemes. In your definition, use the notation $\mathcal{M}$ for the message space and $\mathcal{C}$ for the ciphertext space.
   (b) (3 points) Prove that the one-time pad is a perfectly secret encryption scheme.

2. (5 points) Let F be a pseudorandom function. Let $\|$ denote the concatenation operator, $\oplus$ denote the bitwise XOR operator, and $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i. To authenticate a message $m = m_1 \| m_2 \| \cdots \| m_l$ where $m_i \in \{0,1\}^{n/2}$, suppose that a MAC computes the tag $t = F_k(\langle 1 \rangle \| m_1) \oplus F_k(\langle 2 \rangle \| m_2) \oplus \cdots \oplus F_k(\langle l \rangle \| m_l)$. Show that this MAC is insecure even if we fix l and do not allow truncation attacks. Fixing l implies that the oracle in the $\texttt{Mac-forge}_{\mathcal{A},\Pi}(n)$ experiment can only be queried on messages of length $ln/2$.

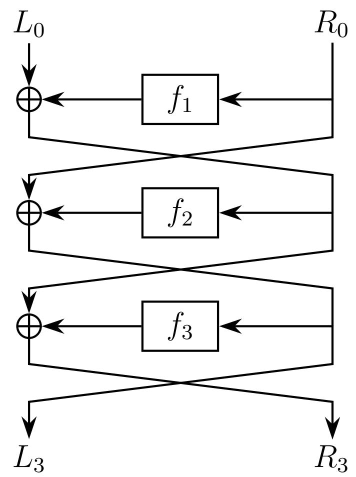
   Hint: A message authentication code $\Pi = (\texttt{Gen}, \texttt{Mac}, \texttt{Vrfy})$ is existentially unforgeable under an adaptive chosen-message attack, or just secure, if for all PPT adversaries $\mathcal{A}$, there is a negligible function $\texttt{negl}$ such that:

$$\Pr\left[\texttt{Mac-forge}_{\mathcal{A},\Pi}(n) = 1\right] \le \texttt{negl}(n).$$

   The message authentication experiment $\texttt{Mac-forge}_{\mathcal{A},\Pi}(n)$ is defined as follows:

   1. A key k is generated by running $\texttt{Gen}(1^n)$.
   2. The adversary $\mathcal{A}$ is given input 1^n and oracle access to $\texttt{Mac}_k(\cdot)$. The adversary eventually outputs (m, t). Let $\mathcal{Q}$ denote the set of all queries that $\mathcal{A}$ asked its oracle.
   3. $\mathcal{A}$ succeeds if and only if (1) $\texttt{Vrfy}_k(m, t) = 1$ and (2) $m \notin \mathcal{Q}$. If $\mathcal{A}$ succeeds, the output of the experiment is 1. Otherwise, the output is 0.

3. (a) (2 points) Give a construction of a CPA-secure private-key encryption scheme for binary messages of length n.
   (b) (2 points) Consider the three-round Feistel network shown below where $L_i, R_i \in \{0,1\}^n$ and $f_i : \{0,1\}^n \mapsto \{0,1\}^n$ are known deterministic functions for $i = 1, 2, 3$. Give expressions for computing L_0, R_0 from L_3, R_3.



(c) (2 points) If an integer x is chosen uniformly from $\mathbb{Z}_{135}$, what is the probability that x belongs to $\mathbb{Z}_{135}^*$? Express your answer in **numerical form**.

(d) (2 points) What is the multiplicative inverse of 13 in $\mathbb{Z}_{135}^*$?

(e) (2 points) Give an example of group G and a subset S of G such that the following conditions are **both** satisfied:

- S is closed under the group operation.
- S is not a subgroup of G.

4. (5 points) State and prove Lagrange's theorem.

5. (5 points) Prove that $n = \sum_{d:d|n} \phi(d)$ where n is an integer greater than one and ϕ is the Euler function. Clearly state any theorems which you use.

6. (5 points) Compute $46^{51} \bmod 55$. Explain the reasoning behind the steps you use.

7. (5 points) Suppose the GenRSA algorithm is used to generate two encryption-decryption exponent pairs (e_1, d_1) and (e_2, d_2) for the same modulus N, where we have $\gcd(e_1, e_2) = 1$. Also, suppose the same message $m \in \mathbb{Z}_N^*$ is encrypted via plain RSA using both the exponents to get ciphertexts c_1, c_2 given by

$$c_1 = m^{e_1} \bmod N,$$
$$c_2 = m^{e_2} \bmod N.$$

Show how a PPT adversary can recover m from c_1, c_2.

8. (a) (3 points) An element $x \in \mathbb{Z}_N^*$ which satisfies $x^{N-1} \neq 1 \bmod N$ is said to be a *witness* that N is composite.

For a given N, suppose there exists a witness that N is composite. Prove that at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite.

(b) (2 points) For an odd integer N, let $N - 1 = 2^r u$ where u is odd and $r \geq 1$. An integer $x \in \mathbb{Z}_N^*$ is said to be a *strong witness* that N is composite if

(i) $x^u \neq \pm 1 \bmod N$ and

(ii) $x^{2^i u} \neq -1 \bmod N$ for all $i \in \{1, 2, \ldots, r-1\}$.

If $x \in \mathbb{Z}_N^*$ is a witness, prove that it is also a strong witness.