EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Endsem Exam : 40 points April 26, 2019

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 length-preserving pseudorandom function having key length, input length, and output length all equal to n bits. Let $\|$ denote the concatenation operator, $\oplus$ denote the bitwise XOR operator, and $\langle i \rangle$ denote an $n/2$-bit encoding of the unsigned 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 $ln/2$. Assume that l satisfies $1 \leq l \leq 2^{\frac{n}{2}} - 1$, i.e. it can be represented as an $\frac{n}{2}$-bit string.

3. (5 points) Recall that the PKCS #5 padding scheme is used to pad a message x having length some integral number of bytes into a *encoded data* m having length jL bytes where L is the block length in bytes. The number of bytes which are appended to x to get m is b where $1 \leq b \leq L$. Each of these padding bytes is equal to the byte representation of the integer b. Assume that $L < 256$.

   Suppose the encoded data m has length $2L$ bytes, i.e. $m = (m_1, m_2)$ where $|m_i| = L$ bytes for $i = 1, 2$. Recall that the encoded data m is obtained by padding the message x. Let F be a length-preserving pseudorandom permutation where $F_k : \{0,1\}^n \mapsto \{0,1\}^n$ where $n = 8L$. (***Note:*** *$8L$ bits $= L$ bytes*)

   Now suppose the encoded data is encrypted using CBC mode as described below.

   - The ciphertext corresponding to $m = (m_1, m_2)$ is given by $c = (c_0, c_1, c_2)$ where
     - c_0 is uniformly chosen from $\{0,1\}^n$.
     - $c_i = F_k(m_i \oplus c_{i-1})$ for $i = 1, 2$.

   Suppose an adversary has access to a padding oracle. On input some ciphertext block $c' = (c'_0, c'_1, c'_2)$, the padding oracle only returns a message from the set $\{\texttt{ok}, \texttt{padding\_error}\}$. The `ok` is returned when there is no padding error in the encoded data m' obtained from c'. If there is a padding error, then `padding_error` is returned.

   Describe a procedure by which the adversary can recover the **length** b of the padding in the encoded data m. Be specific about the inputs sent to the padding oracle and the decisions made by your procedure on receiving the oracle's responses.

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

5. (5 points) For $N > 1$, we know that $\mathbb{Z}_N^*$ is a group under multiplication modulo N. Prove that $a^{\phi(N)} = 1 \bmod N$ for any $a \in \mathbb{Z}_N^*$ where $\phi(N)$ is the Euler phi function.

   Note: $\phi(N)$ is the cardinality of $\mathbb{Z}_N^* = \{b \in \{1, 2, \ldots, N-1\} \mid \gcd(b, N) = 1\}$

6. (5 points) Find x in $\mathbb{Z}_{385}$ which satisfies

   $$\begin{aligned} 3x &= 2 \bmod 5, \\ 4x &= 3 \bmod 7, \\ x &= 2 \bmod 11. \end{aligned}$$

Hint: $385 = 5 \times 7 \times 11$. Note that the left hand sides of the first two congruences have $3x$ and $4x$. You can assume the results of the general Chinese Remainder Theorem without proof, i.e. for integers p_1, p_2, p_3 which are pairwise relatively prime we have $\mathbb{Z}_{p_1 p_2 p_3} \simeq \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3}$ and $\mathbb{Z}^*_{p_1 p_2 p_3} \simeq \mathbb{Z}^*_{p_1} \times \mathbb{Z}^*_{p_2} \times \mathbb{Z}^*_{p_3}$

7. (5 points) We say that $x \in \mathbb{Z}^*_N$ is a *square root of 1 modulo N* if $x^2 = 1 \bmod N$. Prove that if N is an odd prime, then the only square roots of 1 modulo N are 1 and $N - 1$.

8. (5 points) Prove the following: Let $N > 1$ be an odd number that is not a prime power. Then at least half the elements of $\mathbb{Z}^*_N$ are strong witnesses that N is composite.

   Definition of strong witness: 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 $i \in \{1, 2, \ldots, r-1\}$.