Mid Semester Examination

Principles of Information Security
IIIT Hyderabad, Spring 2024

February 27, 2024

There are 9 questions, 10 marks each. Maximum Marks: 90. Time: 90 min

---

1. Consider a modification of the substitution cipher, where instead of applying only the substitution, we first apply a substitution and then apply a shift cipher on the substituted values. Give a formal description of this scheme and show how to break the substitute and shift cipher. Upto what message space size is your scheme perfectly secret?

2. **Negligible or not?** (in each of the following three cases): Let $f, g : \mathbb{N} \to \mathbb{R}$ be negligible functions, let $p : \mathbb{N} \to \mathbb{R}$ be a polynomial such that $p(n) > 0$ for all $n \in \mathbb{N}$. $3 + 3 + 4 = 10$

   1. $h : \mathbb{N} \to \mathbb{R}$ as $h(n) = f(n) + g(n)$.
   2. $h : \mathbb{N} \to \mathbb{R}$ as $h(n) = f(n) \cdot p(n)$.
   3. $f(n) := f'(n) \cdot p(n)$, for some negligible function $f'(n)$ and some polynomial function $p(n)$. Is such a $f(n)$ always negligible?

3. **PRG or not?**: Let $G : \{0,1\}^{2n} \to \{0,1\}^{2n+1}$ be a pseudorandom generator (PRG). For each part below, either prove or disprove that $G' : \{0,1\}^{2n} \to \{0,1\}^{2n+1}$ is *necessarily* a PRG no matter which PRG G is used.

   1. $G'(x) := G(\pi(x))$ for, where $\pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is any poly(n)-time computable bijective function. (You may not assume that π^{-1} is poly(n)-time computable.)
   2. $G'(x||y) := G(x||x \oplus y)$, where $|x| = |y| = n$.
   3. $G'(x||y) := G(x||0^n) \oplus G(0^n||y)$, where $|x| = |y| = n$.
   4. $G'(x||y) := G(x||y) \oplus (x||0^{n+1})$, where $|x| = |y| = n$.

4. Let F be a block cipher (a strong PRP) with 128-bit input length. Prove that neither of the following encryption schemes are CPA-secure: $5 + 5 = 10$

   - Scheme A: choose a random 128-bit r and let $c = \langle r, F_r(k) \oplus m \rangle$. m is of 128 bits.
   - Scheme B: For 256-bit messages: to encrypt message $m_1 m_2$ using key k (where $|m_1| = |m_2| = 128$), choose random 128-bit r and compute the ciphertext $\langle r, F_k(r) \oplus m1, F_k(m_1) \oplus m_2 \rangle$.

5. Prove that the basic CBCMAC is not secure when we consider the messages of different lengths (you need to show an attack). Can you modify the basic CBCMAC for variable length messages to make it secure? Explain in detail. Does the security of CBCMAC depend on the IV? $5 + 3 + 2 = 10$

6. Show that the CBC and Counter modes of operation for block-ciphers are not CCA-secure.

7. Given a family of fixed length collision resistant hash functions $h^s : \{0,1\}^{(n+1)} \to \{0,1\}^n$, show how to build a family of collision resistant hash function H^s for arbitrary length messages $H^s : \{0,1\}^* \to \{0,1\}^n$, using the Merkle-Damgard transform and prove its security. How would you go about building H^s if you are given two functions $h_1^s : \{0,1\}^{(n+1)} \to \{0,1\}^n$ and $h_2^s : \{0,1\}^n \to \{0,1\}^{(n-1)}$ where one of them is collision-resistant family of hash functions, and you do know which one? $7 + 3 = 10$

8. Prove that for a prime p, if $(p-1) = s2^r$ for some odd number s, then the $(r+1)^{th}$ `lsb` (that is the bit that says whether $x \bmod 2^{r+1}$ is $\geq 2^r$) is a hard-core predicate for discrete logarithm in $\mathbb{Z}_p^*$. Using ths hardcore predicate, design a provably secure PRG assuming DLP is hard in $\mathbb{Z}_p^*$. $7 + 3 = 10$

9. If $2^n + 1$ is an odd prime for some integer n, prove that n is power of 2 (such primes are called Fermat primes, examples include 5 and 17). Design an *efficient* algorithm to compute discrete logatirhm in $\mathbb{Z}_p^*$ where p is a Fermat prime. $4 + 6 = 10$