POIS Quiz 1 **29 January 2024**

1. Prove or disprove the negligibility of the following functions:

   (a) $\frac{2^{-1000}}{n}$

   (b) $\frac{1}{(logn)!}$

   (c) $\frac{1}{(\log \log n)!}$ x

   (d) $2^{\frac{-n}{1000}}$

[10]

2. Using your experience in security definitions, provide a definition for perfect pseudorandom generators $G : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$. Furthermore, prove that such perfect PRGs do not exist. [10]

3. Assuming that DLP is hard in Z_{17}^* (of course, it isn't really), using 4-bits to represent each of its elements, design a corresponding PRG $G : \{0,1\}^4 \rightarrow \{0,1\}^*$, and output the first six bits if seed is set to be the last 4 bits of your choice (say, the last 4 bits of the last 2 digits of your roll number). [10]

4. Prove that the shift cipher is perfectly secret as long as only one character in $[a, \ldots, z]$ is encrypted. [10]

End Semester Examination

Principles of Information Security
IIIT Hyderabad, Monsoon 2022

April 29, 2024

There are 10 questions, 10 marks each. Maximum Marks: 100. Time: 180 min

---

1. Recall that the one-time pad is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^n$ and $\mathrm{Enc}(k, m) = k \oplus m$. Notice that when the key $k = 0^n$ is used, then $\mathrm{Enc}(k, m) = m$ and this does not "seem" secure. Suppose we "improve" the one-time pad by setting the key space to $\mathcal{K} := \{0,1\}^n \setminus 0^n$. That is, we take 0^n out of the key space so that it will never be chosen as a key. Does the resulting cipher have perfect secrecy? Justify your answer. More generally, while there is a need for always using only *strong* passwords, is there a need for an analogous notion of *strong* keys for (a) perfect security and (b) computational security. $3 + 3 + 4 = 10$ marks

2. Let $\mathcal{G}$ be a group of prime order p with generator $g \in \mathcal{G}$. Assume that the discrete log problem is hard in $\mathcal{G}$. Consider the following PRG defined over $(\mathcal{Z}_p, \mathcal{G}^2)$: given an input $x \in \mathrm{Z}_p$, the PRG outputs $G(x) := (g^{4x}, g^{5x}) \in \mathcal{G}^2$. Is this a secure PRG? Justify. Using the notion of hard-core predicates, how would you design a secure PRG is the above setting? $6 + 4 = 10$ marks

3. Define (in the way you find appropriate) the notions of (a) *perfect one-way functions* (b) *perfect pseudorandom generators*, (c) *perfect pseudorandom functions*, (d) *perfect collision-resistant hashing* and (e) *perfect public-key cryptosystems* and prove that none of them exist. $5 \times 2 = 10$ marks

4. Does counter mode encryption require a PRP or is a PRF sufficient? Justify your answer. Imagine a new mode of operation for block ciphers for each of the following: $4 + 1\frac{1}{2} \times 4 = 10$ marks

   - It is *insecure* for encrypting *some* (but not all) messages.
   - It is *secure* for encrypting *all* messages of given fixed length ℓ but is insecure for all the other length messages.
   - It is always *insecure* for encrypting each and every message.
   - It is *secure* for encrypting sufficiently long messages, but is insecure for short messages.

5. Design a new MAC scheme that is provably secure (and prove it under CDH/DDH/DLP-assumption) – in more detail, construct a fixed length collision resistant hash function using DLP, followed by the Merkle-Damgard transform and subsequently a HMAC-like design. Compare/contrast your design with the CBCMAC, and which of the two is likely to have a smaller block-size? $3 + 2 + 2 + 2 + 1 = 10$

6. Show that if H_1 and H_2 are distinct collision resistant functions with range $\mathcal{T} := \{0,1\}^n$, then $H(x) := H_1(x) \oplus H_2(x)$ need not be collision resistant. No matter how good the hashing algorithm, prove that to find two passwords that have the same n-bit hash value (colllision) it is expected to take only $O(\sqrt{2^n})$ trials (the Birthday attack rather than brute-force approach of $O(2^n)$ trials). Do you think an OS that uses a 64-bit password hashes are secure with today's technology (argue with time calculations). What is the `hash-and-sign` paradigm? Show that the textbook RSA signatures are *not* secure. Illustrate how the above paradigm enables to tighten RSA-signatures. $2 + 3 + 2 + 1 + 1 + 1 = 10$

7. In 1-out-of-2 Oblivious Transfer (OT), a sender has two message bits $m_0, m_1 \in \{0,1\}$, and a receiver has a choice bit $b \in \{0,1\}$. The sender wants to send m_b to the receiver while satisfying correctness (the receiver obtains m_b), sender's privacy (the receiver gains no knowledge about the message m_{1-b}), and receiver's privacy

(the sender gains no knowledge about the choice bit b). In this problem, we focus on achieving security against *honest-but-curious* senders and receivers.

$5 + 5 = 10$ marks

- Show how you can use any 1-bit OT scheme to build an ℓ-bit OT scheme for transferring ℓ-bit messages $m_0, m_1 \in \{0,1\}^\ell$. Here $\ell = \ell(\lambda)$ is a (possibly large) polynomial in security parameter λ. Your scheme can only invoke the given 1-bit OT scheme at most $\lambda \ll \ell$ times. You can assume the existence of a pseudorandom generator.
- A 1-out-of-n secret sharing scheme is one where the sender has n messages $m_0, \ldots, m_{n-1} \in \{0,1\}^\ell$ and the receiver wants the i^{th} message m_i.

  You are given a 1-out-of-2 OT scheme with ℓ-bit messages. Show how to construct a 1-out-of-n OT scheme for any integer $n \geq 2$. You can assume the existence of a PRF family. For full credit, your scheme must invoke the 1-out-of-2 OT scheme at most $O(\log n)$ many times.

8. A prime p is called b-smooth if all the prime factors of $(p-1)$ are at most b. Design an algorithm that is polynomial-time is $\log b$ to compute discrete logatirhm in $\mathbb{Z}_p^*$ where p is b-smooth. What kind of primes p have the maximum value of b (relative to p), and are better suited for DLP-based cryposystems like the El Gamal public-key cryptosystem (PKC)? Under DDH, prove that El Gamal PKC is CPA-secure. Prove that El Gamal PKC is *not* CCA-secure. Show how would to design a new provably CCA-secure PKC starting with the El Gamal PKC. $5+1+2+1+1 = 10$

9. For each of the following statements, say whether it is *true* or *false*, with proof. $2 \times 5 = 10$ marks

   - There exists a pseudorandom generator $G = \{G_n\}$ where for every n, $G_n : \{0,1\}n \to \{0,1\}^{2n}$ such that for every $x \in \{0,1\}^n$, the first $n/3$ bits of $G_n(x)$ are zero.
   - There exists a pseudorandom generator $G = \{G_n\}$ where for every n, $G_n : \{0,1\}n \to \{0,1\}^{2n}$ such that for every $x \in \{0,1\}^n$, if the first $n/3$ bits of x are zero then all the bits of $G_n(x)$ are zero (i.e., $G_n(x) = 0^{2n}$).
   - There exists a pseudorandom function collection $\{f_s\}_{s \in \{0,1\}^*}$ where, letting $n = |s|$, $f_s : \{0,1\}^n \to \{0,1\}^n$ *that satisfies the following:* for every $s \in \{0,1\}^! n$, $f_s(0^n) = 0^n$.
   - For $\ell \geq 2$ and a string $x \in \{0,1\}^\ell$, let *cnot* : $\{0,1\}^\ell \to \{0,1\}^\ell$ be the following function: $cnot(x_1, \ldots, x_\ell) = x_1, x_2 \oplus x_1, x_3, \ldots, x_\ell$. (That is, *cnot* flips the second bit of x according to whether or not the first bit is one.) There exists a CPA-secure public key encryption scheme (Gen,Enc,Dec) and a polynomial time algorithm A, such that for every n, if $(e,d) = \text{Gen}(1^n)$ then for every $x \in \{0,1\}^\ell$ (where ℓ is the message size of the encryption scheme for security parameter n) it holds that

     $$\text{Dec}_d\Big(A\big(e, \text{Enc}_e(x)\big)\Big) = cnot(x)$$

   - Repeat the above for CCA-secure public key encryption scheme.

10. Write in detail about any <u>two</u> of the following: $2 \times 5 = 10$

    1. Blockchains
    2. Efficient Quantum Algorithm for Integer Factorization
    3. Quantum Secure Key Establishment
    4. Quantum Teleportation
    5. Chinese Remainder Theorem
    6. Byzantine Agreement
    7. Digital Certificates and PKI •
    8. Random Oracle Model
    9. Secret sharing •
    10. Perfectly Secure Multiparty Computation

BEST OF LUCK