End Semester Examination

Principles of Information Security
IIIT Hyderabad, Monsoon 2022

April 29, 2023

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

---

1. For each of the following historical ciphers, either show how to break them or prove their unbreakabilty by using Shannon's perfect secrecy: $2 \times 5 = 10$
    1. Caesar Cipher
    2. Shift Cipher
    3. Mono-Alphabetic Substitution Cipher
    4. Vegenere Cipher
    5. Vernam Cipher (one-time pad)
2. Formally define the concept of negligible functions. Give an example or prove *the non-existence of* an operation $\circ$ on functions for each of the following: $2 \times 5 = 10$
    1. Negligible functions are closed under $\circ$ and non-negligible functions are closed under $\circ$. ×
    2. Negligible functions are closed under $\circ$ and non-negligible functions are not closed under $\circ$. %
    3. Negligible functions are not closed under $\circ$ and non-negligible functions are closed under $\circ$. −
    4. Negligible functions are not closed under $\circ$ and non-negligible functions are not closed under $\circ$. +
    5. If f is negligible and g is non-negligible then $f(n) \circ g(n)$ is neither always negligible nor always non-negligible. ×
3. Prove each of the following: $4 + 3 + 3 = 10$
    1. Define (in the way you find appropriate) the notions of *perfect one-way functions* and *perfect pseudorandom generators* and prove that neither of them can actually exist.
    2. Formally define *one-way functions* and *pseudorandom generators* and prove that one-way permutations imply pseudorandom generators.
    3. Define *pseudorandom functions* and prove that they exist if pseudorandom generators exist.
4. What is the need for probabilistic encryption? How to easily achieve probabilistic encryption provided *the ciphertext can be double the size of the plaintext*? Illustrate a couple of secure modes of operation *of block ciphers (that resolve the length-doubling problem)* and compare them in detail. Imagine a *new mode of operation* for block ciphers for each of the following: $1 + 2 + 3 + 1 \times 4 = 10$
    1. It is *insecure* for encrypting *some* (but not all) message.

2. It is *secure* for encrypting *all* messages of given fixed length ℓ but is insecure for all the other length messages.
3. It is always *insecure* for encrypting each and every message.
4. 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) — specifically, 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. 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 for a Birthday attack). 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. $4+2+1+2+1 = 10$

7. Describe a *zero knowledge proof* (ZKP) for GRAPH-3-COLORING (G3C). Prove the completeness, soundness and the zero-knowledgness of your protocol/proof. Why are digital signatures a special case of zero-knowledge proofs? Can you imagine a new kind of interactive authentication protocol based on the the hardness of GRAPH-3-COLORING and your ZKP for it? $3+3+1+3 = 10$

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. Show how to solve the problem of *oblivious transfer* (OT) in the following settings: $3+4+3 = 10$
   1. Assuming secure PKC exists.
   2. Using channel noise, even if one-way functions do not exist.
   3. If there are three parties (one among them is passively corrupt by a computationally unbounded adversary) and OT is to be done between two of them.

10. Write in detail about any *two* of the following: $2 \times 5 = 10$
    1. Kerckhoff's Principle
    2. Shannon's Theory of Perfect Secrecy
    3. Impagliazo's Five Possible Worlds From Algorithmica to Crypyomania
    4. Fiat-Shamir Heuristic for Designing Non-interative ZKP
    5. Details of any two Public-key Cryptosystems (other than RSA and El Gamal)
    6. Advanced Encryption Standard (AES)
    7. Feistel Networks and converting PRF to PRP.
    8. Random Oracle Model and RSA-OAEP
    9. Shamir's secret sharing and General Secret Sharing over Access Structures
    10. General Secure Multiparty Computation

BEST OF LUCK