CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

End Semester Examination

Due by: May 14, 2021 23:55 PM

Max Marks: 60

Instructions.

- Solutions should be mandatorily LaTeXed using the template shared and submitted through GradeScope before time. Mention Group Numbers and member names in solutions (refer template instructions).
- Clearly express solutions avoiding unnecessary details. Everything discussed in class is not required to be proved again. And anything non-trivial must be proved.
- Write the solutions on your own. Acknowledge the source wherever required. Keep in my mind department's Anti-Cheating Policy.

Question 1. (25 marks) Anubha and Braj were partners of a multinational company but due to some misunderstanding, they decided to part ways with one another. In order to split the numerous assets of the company, they came forward with the following plan.

- For each asset, Anubha would first toss a coin and record its outcome but does not share it with Braj.
- Braj would then try to guess the outcome. If he guesses the outcome of the toss correctly, he will own that asset. Otherwise, Anubha will get the asset.

Observe that this scenario has a flaw. Anubha can always lie to about the outcome of the toss. For this reason, Braj comes up with another plan.

- Anubha would first toss the coin and record the outcome as a bit b (i.e., $b = 0$ if outcome is heads else $b = 1$). She then randomly chooses a matrix $A \in \mathbb{Z}_q^{n \times m}, m >> n$ and $r \in \{0,1\}^{m-1}$ and sends $c = A[b|r]^T \; mod \; q$ and A to Braj.
- Braj will try to guess b and shares his guess with Anubha. After sharing his guess, Anubha will share b, r with Braj, so that he can verify that Anubha is not cheating.

1. Show that if Anubha is able to cheat, i.e., she can send b', r' to Braj claiming that $c = A[b'|r']^T$ where $b' \neq b$, then she can solve some approximation of Shortest vector problem in some lattice.
2. Give an argument why it is hard for Braj to find any valid b' from c.

Question 2. (10 marks) A cryptographic hash function h takes as input a message of arbitrary length and produces as output a message digest of fixed length, for example 160 bits. Certain properties should be however satisfied:

- Given a message m, the message digest $h(m)$ can be calculated very quickly.
- Given a message digest y, it is computationally infeasible to find an m with $h(m)$ = y(in other words, h is a one-way, or preimage resistant function).
- It is computationally infeasible to find messages m_1 and m_2 with $h(m_1)$ = $h(m_2)$ (in this case, the function h is said to be strongly collision-free).

Argue that the hash function $h(m)$ = $g^m \mod p$ where p is a large prime and g is a generator of $\mathbf{F}_p^*$ cannot be used.

Question 3. (10 marks) Anubha and Braj agreed on a following key-exchange protocol:

- Anubha chooses uniform $k, r \in \{0,1\}^n$, and send $s := k \oplus r$ to Braj.
- Braj chooses uniform $t \in \{0,1\}^n$, and send $u := s \oplus t$ to Anubha.
- Anubha computes $w := u \oplus r$ and send w to Braj.
- Anubha outputs k and Braj outputs $w \oplus t$.

Show that Anubha and Braj output the same key. Analyse the security of this protocol.

Question 4. (15 marks) Let $N = p \cdot q$ be RSA modulus such that $\frac{1}{2}N^{1/2} < p, q < 2N^{1/2}$. Suppose prime p has ℓ bits. Show that if $\ell/2$ most significant bits of p are known then N be factored in $O(\log N)$ time.
