CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

End Semester Examination

Group Number: PolkaDots
Yatharth Goswami (191178), Rohan Baijal (190714), Sarvesh Chandra (190773)

Date of Submission:
May 14, 2021

Question 1

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 Bob.
- 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, Bob comes up with another plan.

- Alice 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 Alice. After sharing his guess, Alice 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 Bob to find any valid b' from c.

Solution

Notice that since b is obtained from a coin-flip so it can be considered a random bit. Therefore the vector $[b|r]$ is a random vector with entries in $\{0,1\}$. Now, consider the lattice formed by vectors which are in null space of matrix A. This corresponds to the set $\lambda = \{y \in \mathbb{Z}_m : Ay = 0 \mod q\}$. Consider the lattice formed by elements in the set λ.

Now, A is a random matrix and suppose we want to find short vectors in the lattice formed by λ as defined in the previous paragraph. First let us try to estimate the determinant of the basis of lattice formed by . In [1], the authors show that the determinant of this lattice can be approximated to be less than q^n.

Now, applying Minkowski's theorem we get that the shortest vector (x) is bounded by

$$x \leq \sqrt{m}(det(\lambda))^{1/m} \leq \sqrt{m}q^{n/m}$$

- Now, suppose Alice is able to find another b' and r' such that $A[b'|r']$ is same as $A[b|r]$ modulo q. Let $x = [b|r]$ and $x' = [b'|r']$. Now we can say that

  $$A(x - x') = 0 mod q$$

  Let $v = x - x' \in \mathbb{Z}_m$, notice the fact that vector v has small entries from the set $\{-1, 0, 1\}$ and hence the norm of this vector is atmost $\sqrt{m}$. Therefore using the bound found using Minkowski's theorem this v is a short vector for lattice formed using λ. Hence, if Alice finds such a v, then she can actually find the shortest vector of this lattice. Now, A being random leads to the fact that Alice can solve the SVP problem for any random lattice, which is equivalent to solving this worst case hard lattice problem. Hence, the technique is safe to use. Hence, finding another b' is very difficult and this makes the function collision resistant.

- The second part required us to show that it is difficult for bob to find any solution b' to this problem. We can claim that finding such a solution is equivalent to breaking the collision resistant behaviour of the funciton which using the above argument is shown to be hard for the current scenario. Assume that bob succeeds in finding a solution b' such that it produces the same c. Notice that, if $b' \neq b$, then bob is actually able to find a collision and hence breaks the collision resistant property of

the original function. We can show that with very high probability $b \neq b'$ since the hash function is a shrinking function in nature and maps arbitrarily long texts to shorter ones ([2]). Hence proved that it is difficult to find such a b' for bob.

Question 2

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.

Solution

The hash function $h(m) = g^m \ mod \ p$ satisfies the 1st and 2nd properties, but not the 3rd.
Property 1 : It is easy to see that given a message m, the hash can be computed in $O(logm)$ time, hence it is pretty quick.
Property 2 : We know that given y, it is a hard problem to find m such that $h(m) = y \ mod \ p$ since this is the Discrete Log Problem.
Property 3 : The function fails to satisfy this property. We know that $p - 1$ is the order of the group. Hence, m and $m + p - 1$ will produce the same digest.
$g^{m+p-1} \ mod \ p = ((g^m \ mod \ p).(g^{p-1} \ mod \ p)) \ mod \ p = g^m \ mod \ p$.

Question 3

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.

Solution

Given : $s := k \oplus r$, $u := s \oplus t$, $w := u \oplus r$.
Anubha already has k.
Now, Braj outputs $w \oplus t = (u \oplus r) \oplus t = ((s \oplus t) \oplus r) \oplus t = (((k \oplus r) \oplus t) \oplus r) \oplus t = k$.
Hence, both output the same key.

Notice that as an eavesdropper, I have access to s, u *and* w.
Now $s \oplus u \oplus w = k$.
The $\oplus$ operation takes $O(n)$ time where n is the length of the bit string. Hence, an attacker can retrieve the key k in $O(n)$ time.

Question 4

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.

Solution

References

[1] Short vectors in q-ary matrices. https://homes.esat.kuleuven.be/~nsmart/FHE-MPC/Lecture2.pdf.

[2] Collision resistant implies one-wayness. https://crypto.stackexchange.com/questions/71966/collision-resistant-hash-function-implies-one-way-function.