Homework 2 - Cryptography

Foundations of Blockchain Technology and cryptocurrencies

Fall 2019

Sharif Blockchain Lab
Sharif University of Technology
Department of Electrical Engineering

Deadline: Yekshanbeh 1398/8/12 At the beginning of the class

(The Homeworks will be collected at the beginning of the class. 3 minutes after the start of the class the homeworks will not be accepted).

Section 1) Hash functions

1. **(3 points) a.** Prove that if a hash function is collision resistant it is also 2nd-preimage resistant.

   (2 points) b. Prove that if a hash function is 2nd-preimage resistanct it will not imply that it is also preimage resistant. (Give counter example).

   (2 points) c. What can we say about the relationship between pre-image resistance and collision resistance? Can we imply anyone from the other one? If not please provide counter example and if yes provide a proof.

2. **part 1) (6 points, 2 points each)** Let H_1 and H_2 be two hash functions. We know that at least one of these hash functions is collision-resistant. We construct new hash functions using H_1 and H_2 as shown in $(a), (b)$ and (c). Which one is collision resistant? Prove it! If it is not collision resistant, then find a collision for each H.

   (a) $H_a(x) \coloneqq H_1(x)||H_2(x)$

   (b) $H_b(x) \coloneqq H_1(H_2(x))||H_2(H_1(x))$

   (c) $H_c(x) \coloneqq H_1(H_2(x)||x)||H_2(H_1(x)||x)$

   part 2) (3 points) If T is a collision resistant hash function what can we say about $T_1(x) \coloneqq T(x) \oplus T(x \oplus 1^{|x|})$? (i.e., $x \oplus 1^{|x|}$ is the complement of x. e.g., the complement of 1101 is 0010). If it is collision resistant prove it. Otherwise find a collision.

Section 2) Merkle tree

3. By using binary merkle tree Arman can commit to a set of files $S = \{F_1, F_2, F_3, ..., F_n\}$ that later he can prove to Rasoul that a file F_i is in the set (This process is called proof of inclusion that as it was shown in the class it can be shown by $O(\,log(n)\,)$ hashes).Commit means Now suppose that the merkle tree is not binary and is a k-ary tree. k-ary tree means every non-leaf

node has up to k children. The hash value of each non-leaf node j is computed as the hash of the concatation of all j's children.

(a) **(10 points)** Suppose there are 10 files in the set S. How can Arman compute the commitment to S using a 3-ary merkle tree? How can Arman prove to Rasoul that F_5 is in the set S?

(b) **(7 points)** Suppose S contains n Files. What is the length of proof (i.e., number of hashes) which proves that some F_i is in the set S? (Give a function using n and k, in a k-ary tree).

(c) **(7 points)** What is the best choice for k if n is a large number?

4. **(10 points)** By using a merkle tree we can provide a proof for existence of a file. What if you want to prove a specific file **does not** exist in a set of files? How can we do that using a merkle tree? (**Hint:** Read about sorted merkle tree).

Section 3) Elliptic curve

5. **(11 points)** We have seen how to perform key exchange in Elliptic curve. i.e., Diffie-Hellman using elliptic curves. Explain how encryption and decryption works in elliptic curve. Provide one example (You can use this link to study about elliptic curve encryption). Also search about digital signature using elliptic curve (i.e., ECDSA) and explain how it works.

Section 4) RSA

6. Recall the RSA method with the same notation in the slides of the class for $N, p, q, \varphi(N), e, d$.

(7 points) a) By having a (public-key,private-key) pair in RSA how can we efficiently factorize N? In other words how can we efficiently factorize N by having e, d, N?

(3 points) b) Imagine a company wants to give each employee a different pair of keys $(e, d)(N$ is the same for all pairs). Show that in this company any employee can decrypt any message encrypted by other employees. So there is no privacy! (**Hint:** Use part a)

(5 points) c) We claimed that we have to keep $\varphi(N)$ secret in RSA. How can we attack RSA cryptosystem if we know $\varphi(N)$ and a public key?(public-key = (e, N))

Section 5) Applications

7. Arman and Rasoul are talking on phone, discussing about where to go in the evening. Arman suggests to go bowling but Rasoul suggests to go hiking. They discuss about it but they can not come up with a conclusion. To solve the problem, Arman picks a coin to play lion-or-line!! game (i.e., "Shir ya Khat" instead of head-or-tail) with a fair coin.

Arman: "OK, Lets play lion-or-line! I will toss the coin, and you tell me if it is lion or line. If you win we will do what you suggest, Otherwise we will go bowling."

Rasoul: "It is a good idea but I can not see the coin. How can I trust you ?"

(6 points) Question: Can you suggest a protocol in which they can do this and cheating is "hard" for any of them? (**Hint:** Think of a commitment scheme using hash. But be careful because it is not as simple as it seems! There is one small twist).

8. Arman and Rasoul are living in a country with 60 cities $\{c_1, c_2, ..., c_{60}\}$. Arman is living in city $a \in \{c_1, c_2, ..., c_{60}\}$ and Rasoul is living in city $b \in \{c_1, c_2, ..., c_{60}\}$. They are talking on phone and Arman is willing to know if Rasoul lives in the same city as him.
If Rasoul is living in the same city as Arman, Arman want to understand it, But if Rasoul is living in another city, Arman should not be able to understand b. Also in this process Rasoul should not learn any data about Arman's city.

   i. They agree on a group G of order p (p is a prime number) and a generator g.
   ii. Arman chooses two random values $x, y \in Z_p$ and sends Rasoul $(A_0, A_1, A_2) = (g^x, g^y, g^{xy+a})$
   iii. Rasoul chooses random values $r, s \in Z_p$ and sends Arman $(R_1, R_2) = \Big(A_1^r g^s\ ,\ (\frac{A_2}{g^b})^r A_0^s\Big)$

   (11 points) Question a) How can Arman understand if $a = b$?
   (7 points) Question b) Why Rasoul can not learn anything about a?

Section 6) Kilian's Randomization

9. Assume that you have $\{A_{1,0}, A_{1,1}\}, \{A_{2,0}, A_{2,1}\}, ..., \{A_{kn,0}, A_{kn,1}\}$ in which A_{ij} s are all invertible $L * L$ matrices with elements from F_p. There is a natural function $f : \{0, 1\}^n \to F_p^L * F_p^L$ which takes any n-bit binary input like $b_1, ..., b_n$ and gives $A_{1,b_1} * A_{2,b_2} * ... * A_{nt+r,b_r} * ... * A_{kn,b_n}$ as output. Let $R_1, ..., R_{kn-1}$ be sample random (invertible) matrices and set R_0, R_{kn} to be I. Define $A'_{i,j} = R_{i-1}^{-1} A_{i,j} R_i$ and now you can define f' based on new matrices.

   (5 points) Question a) Prove that f and f' are same functions and then prove that for any binary n-bit array $b_1 b_2 ... b_n$,joint distribution of matrices $A'_{1,b_1}, A'_{2,b_2}, ..., A'_{nt+r,b_r}, ..., A'_{kn,b_n}$ is uniform distribution over all kn-tuples of $L * L$ matrices which their product is $A_{1,b_1} * A_{2,b_2} * ... * A_{nt+r,b_r} * ... * A_{kn,b_n}$
   (3 points) Question b) Describe how this property can help you build a secure program