HYPERLEDGER

EB 20/21	Enterprise Blockchain Technologies	Number:	2
Module I - Introduction		Issue Date:	
Background: Cryptography & Security		Due Date:	

Instructors Guide

This document provides a proposal for a solution for LAB#02, which concerns an introduction to cryptography and security. In particular, the RSA algorithm is introduced. Most of the solutions can be found at [1–3]. Note: You can also experiment with Hyperledger Ursa, a crypto library [1], which supports symmetric encryption and digital signatures.

1 RSA

Exercise 1: How many combinations can the MD5, and SHA256-3 algorithms generate? What is the likelihood of a hash collision with MD5? And with SHA256-3? Is SHA256-3 safer than MD5?

MD5 is a 128-bit cryptographic hash function, which means that digests are distributed over a 128-bit space. MD5 can output 2^{128} digests. Two files should have a $\frac{1}{2^{128}}$ change of collision. However, due to the birthday paradox, that probability would be $\frac{1}{2^{64}}$.

SHA256-3 is a 256-bit cryptographic hash function, which means that digests are distributed over a 256-bit space. SHA256-3 can output 2^{256} different digests. Two files should have a $\frac{1}{2^{256}}$ change of collision. However, due to the birthday paradox, that probability would be $\frac{1}{2^{128}}$.

MD5 is considered to be vulnerable to collision attacks [4].

Exercise 2: Refer to Figures 3 and 4. Is this approach of signing and validating a document secure?

This approach is generally considered secure, given that Alice's public key is authentic (to prevent man-in-the-middle attacks). The hash function that creates the digest is secure. The key distribution should be done securely. See public-key infrastructure, public key certificates, and the X.509 norm.

Exercise 4: Calculate the RSA keys associated with primes $p = 7$ and $q = 29$

Public key is $K_u = (N, e)$ and the private key, $K_r = (N, d)$.

$N = p.q = 7.29 = 203$ $Z = (p-1).(q-1) = 6.28 = 168$ e is chosen such that the greatest common divisor between e and 168 is be one. $e = 5, 11, 13, 17, 19, ...157, 163, 167$. $d = 101$, because 101 is the only number such that $e.d \mod (p-1).(q-1) = 1$. Restriction: $0 < d < (p-1).(q-1)$. The public key $K_u = (N, e)$ is $(203, 5)$ and the private key, $K_r = (N, d)$ is $(203, 101)$.

[1] https://github.com/hyperledger/ursa

EB 20/21	Enterprise Blockchain Technologies	Number:	2
Module I - Introduction		Issue Date:	
Background: Cryptography & Security		Due Date:	

Exercise 5: Given that the public key $K_u = (N, e) = (143, 7)$, encrypt the following message: "P"

P is 80 in ASCII encoding. $C = M^e \mod n = 80^7 mod 143 = 141$.

Exercise 6: Decrypt the criptogram 80, given that $p = 3$ and $q = 31$

$N = p.q = 3.31 = 93$. $d = 43$. The private key is, therefore, $K_r = (N, d) = (93, 43)$. $M = C^d \mod n = 80^4 3 mod 93 = 87$.

References

[1] E. Conrad, S. Misenar, and J. Feldman, "Domain 3: Security Engineering (Engineering and Management of Security)," in *CISSP Study Guide*. Elsevier, jan 2016, pp. 103–217.

[2] P. Rogaway and T. Shrimpton, "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance," Tech. Rep., 2004.

[3] Tecnico Lisboa, "Discrete Mathematics," 2020. [Online]. Available: https://fenix.tecnico.ulisboa.pt/cursos/leic-a/disciplina-curricular/1529008373641

[4] X. Wang and H. Yu, "How to break MD5 and other hash functions," in *Lecture Notes in Computer Science*, vol. 3494. Springer Verlag, 2005, pp. 19–35. [Online]. Available: https://link.springer.com/chapter/10.1007/11426639_2