Portfolio 2 Documentation

CSI2108

James O'Grady

10561121

Task 5

Security Features

For security features in my hashing algorithm, I have implemented 3 different ones to boost the security.

Firstly, I have implemented salting functionality. This helps with pre-image attack resistance as well as second preimage resistance, since the salt that is appended to the input makes it far harder for an attacker to guess an input that matches the given hash.

Secondly, I have implemented multiple rounds of hashing, each subsequent one based off the output of the last one. This increases the diffusion of the hashing algorithm, as an amount of non-linearity that will make it far harder for an attacker to reverse engineer the input when given a hash. This also indirectly increases the collision resistance, since after multiple rounds of hashing a similar input may look completely different.

Thirdly, the use of the previous hashes result and a counter attribute increase the nonlinearity of the algorithm, since the output changes based on the length of the input as well as the content, meaning that although there could exist some value that would produce the same hash, it now also needs to be of the same length or have equivalent total lengths.

Task 6

Alice’s RSA key pair is used to encrypt the hashed messaged digest D from task 5 using her private key. This allows Bob to then decrypt it with her public key. Because she is the only one to have access to her private key, this provides proof of sender, non-repudiation and authentication for the content of the message, since the hash not match if someone has interfered with the message. Bob can decrypt the message and check the hash of it against the hash given.

Task 7

Reflection

Constructing this portfolio and exploring the various cryptosystems that help facilitate modern life was interesting. I wasn’t aware just how much maths affects our daily life and implementing my own versions of cryptographic systems like RSA, stream ciphers and hashing algorithms has been a fun and rewarding experience. I found it very interesting, although difficult, to learn about the maths and how modular arithmetic (which I previously thought was fairly useless) actually plays a large part in keeping everyone safe online. I have previously implemented some rudimentary forms of encryption in python previously but understanding the math behind the algorithms used to secure the modern world have made the algorithms I created far more effective.

The assignment has definitely changed my view on cryptography, moving more toward interest and understanding then my previous vague idea about some of the concepts like symmetric and asymmetric encryption.

References

Extended Euclidean Algorithm. (2023, April 19). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Extended_Euclidean_algorithm&oldid=1150662331#Pseudocode