Hashing and authentication

When data is received, how can the receiver know that it's authentic? Message authentication verifies that the sender possesses the shared secret key and that the data was not altered. The main tool for this process is hashing.

We will see two ways of hashing, one cryptographic and one not, both of which can be embedded in a secure message authentication algorithm (a MAC). We will also see the security model used to claim security.

When both privacy and authentication are desired, one can supply each separately (ie, encrypt a message and then authenticate the ciphertext), but it is safer and faster to combine the two goals into a single operation. Algorithms that intertwine encryption and authentication are called authenticated-encryption algorithms and should be preferred to doing the two operations independentlay.

Learning objectives

By the end of this module you should be able to...

- Calculate the result of a polynomial using divisionless mod and Horner's rule;
- Determine ε for which a collection of hash functions is ε-almost-universal;
- Define preimage-, second-preimage-, and collision-resistance for cryptographic hash functions;
- Explain what it means for a message authentication algorithm to be secure;
- Describe the Merkle-Damgard and Sponge constructions used in cryptographic hash function designs; and
- Describe how at least one authenticated-encryption algorithm safely uses a single key.