One-Way Hash Functions

One-way hash functions are a cryptographic construct with multiple uses. They are used in conjunction with public-key algorithms for both encryption and digital signatures. They are used in integrity checking. They are used in authentication. They are used in communications protocols. Much more than encryption algorithms, one-way hash functions are the workhorses of modern cryptography today.

One-way functions prevent an outsider from taking an existing hash result and determining other data values that match that hash result. Thus, Hector might have received a message saying “I willingly give to Hector my prized golden sponge cake recipe” and some other things. Hector can certainly change “sponge cake recipe” to “bullion collection” but then Hector is stuck: He needs to make other changes to the message, but he needs to know other content that would produce the original hash value. With a one-way function he can guess “recipe file,” “box of pieces of string too short to use,” and so forth. But he has to invent each such phrase and test it. It would be easier if he could run the hash function in reverse and get a list of inputs that would produce a given hash result. Alas, with a one-way function Hector is going to have to keep trying until he finds a match. Modern hash functions must meet two criteria: They are one- way, meaning that they convert input to a digest, but it is infeasible to start with a digest value and infer an input that could have produced that digest. Second, they do not have obvious collisions, meaning that it is infeasible to find a pair of different plaintexts 3 that produce the same digest.

3. Note: Some authors refer to this second property as “collision free,” but that is a misleading term. Every hash function will have collisions−any of them, because the function takes a relatively large input and produces a relatively small digest. It is physically impossible to reduce 512 bits to a 128-bit digest and not have collisions. The point is that the collisions are unpredictable. We know collisions will occur; it is just infeasible to predict which pairs will collide or, given one input, to enumerate other inputs with which the first will collide.

Message Digests

The most widely used cryptographic hash functions are MD4, MD5 (where MD stands for Message Digest), and SHA or SHS (Secure Hash Algorithm or Standard). The MD4/5 algorithms were invented by Ronald Rivest and RSA Laboratories in 1990– 1992. MD5 is an improved version of MD4. Both condense a message of any size to a 128-bit digest. SHA is actually a growing family of algorithms: SHA-0, the original SHA, based on MD4/MD5, was published by NIST in 1993 but was withdrawn shortly thereafter because of an undisclosed " significant flaw." It was replaced by a slightly revised version, known as SHA-1. SHA-1 produces a 160-bit message digest from any input up to 264 bits.

Goodluck ,,,