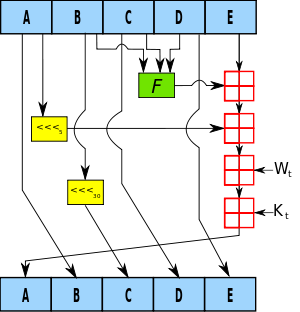
In [cryptography](https://en.wikipedia.org/wiki/Cryptography), **SHA-1** (**Secure Hash Algorithm 1**) is a [cryptographic hash function](https://en.wikipedia.org/wiki/Cryptographic_hash_function) designed by the United States [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) and is a U.S.[Federal Information Processing Standard](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard) published by the United States[NIST](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology).[[2]](https://en.wikipedia.org/wiki/SHA-1#cite_note-:0-2) SHA-1 produces a 160-[bit](https://en.wikipedia.org/wiki/Bit) (20-[byte](https://en.wikipedia.org/wiki/Byte)) hash value known as a [message digest](https://en.wikipedia.org/wiki/Message_digest). A SHA-1 hash value is typically rendered as a [hexadecimal](https://en.wikipedia.org/wiki/Hexadecimal) number, 40 digits long.

[](https://en.wikipedia.org/wiki/File:SHA-1.svg)

One iteration within the SHA-1 compression function:  
A, B, C, D and E are 32-bit [words](https://en.wikipedia.org/wiki/Word_(data_type)) of the state;  
*F* is a nonlinear function that varies;  
[left shift](https://en.wikipedia.org/wiki/File:Lll.png)*n* denotes a left bit rotation by *n* places;  
*n* varies for each operation;  
Wt is the expanded message word of round t;  
Kt is the round constant of round t;  
[Addition](https://en.wikipedia.org/wiki/File:Boxplus.png) denotes addition modulo 232.

SHA-1 produces a [message digest](https://en.wikipedia.org/wiki/Message_digest) based on principles similar to those

the [MD4](https://en.wikipedia.org/wiki/MD4) and [MD5](https://en.wikipedia.org/wiki/MD5)message digest algorithms, but has a more conservative design.

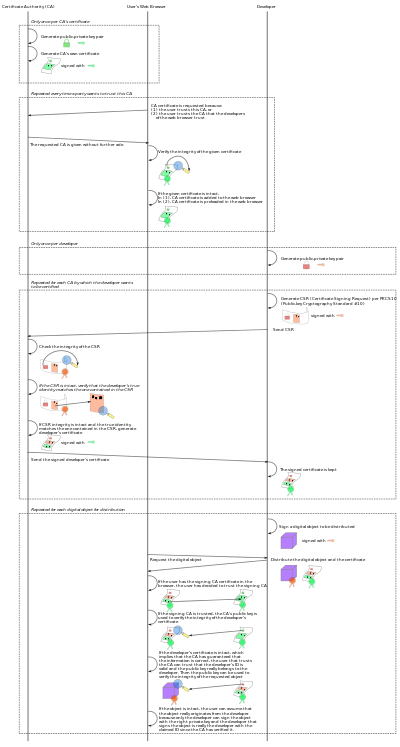
[](https://en.wikipedia.org/wiki/File:Usage-of-Digital-Certificate.svg)

Diagram of an example usage of digital certificate

In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a **public key certificate** (also known as a **digital certificate** or **identity certificate**) is an electronic document used to prove ownership of a[public key](https://en.wikipedia.org/wiki/Public_key).