HASHES AND MESSAGE DIGESTS

Method, application and standards

Features of a Hash Function (I)

- f(message) and normally < length of message
- f(.) is a one way function
- secure if

  - knowing $f(m_1)$ infeasible to find m_2 such that $f(m_1) = f(m_2)$

  - infeasible to find m_1 and m_2 such that $f(m_1) = f(m_2)$

Features of a Hash Function(II)

- f(m) may not be predicted from any part of m
- typical length of f(m) is 128 bits but SHA-1 is 160 bits

Application of Message Digests

- Protection of stored data and programs
- Authentication or MAC generation
- Encryption

Length of secure message digest (Birthday Paradox)

- if more than 23 people in a room then very likely that two will have the same birthday

- if n people in a room and k possible birthdays

there are n(n-1)/2 possible pairs each with prob 1/k of a birthday match

then prob of at least one match is n(n-1)/2k

which is ≈ $n^2/2k \geq 0.5$ if $n \geq \sqrt{k}$

Birthday Paradox and MD length

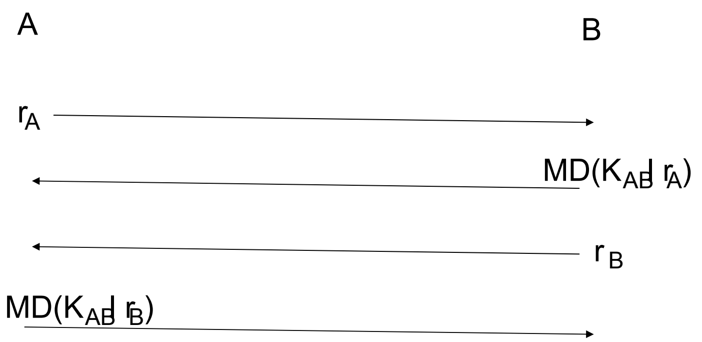
- Let length of message digest be Lbits

then there are 2^L possible message digests

and from the Birthday Paradox $2^{L/2}$ messages should be tested before a match is found

since testing 2^{64} would be infeasible, L should be 128 bits

Authentication with a message digest



MAC Generation

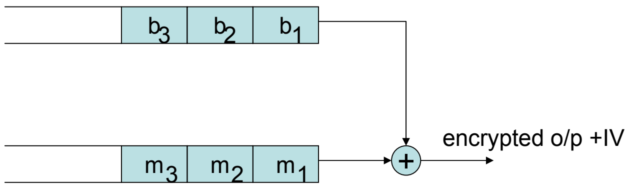
- compute $MD(K_{AB} | m)$

- HMAC uses two hashes

Encryption with a message digest

calculate $b_1 = MD(K_{AB} | IV)$ $c_1 = m_1 \oplus b_1$

$b_2 = MD(K_{AB} | c_1)$ $c_2 = m_2 \oplus b_2$

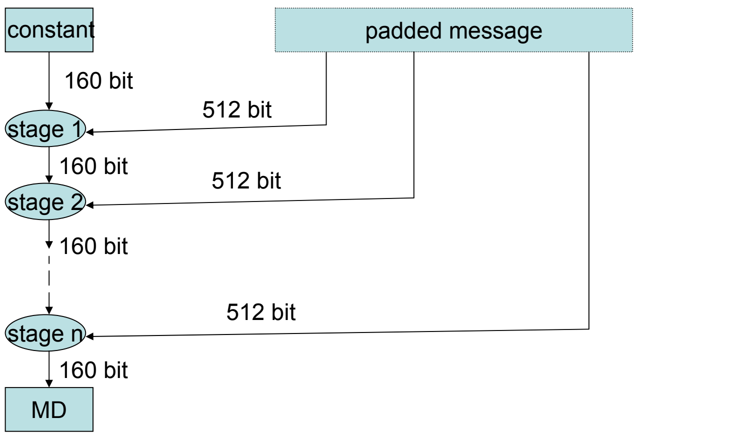


NB For decryption calculate b_i and then $m_i = c_i \oplus b_i$

Message Digest Standards

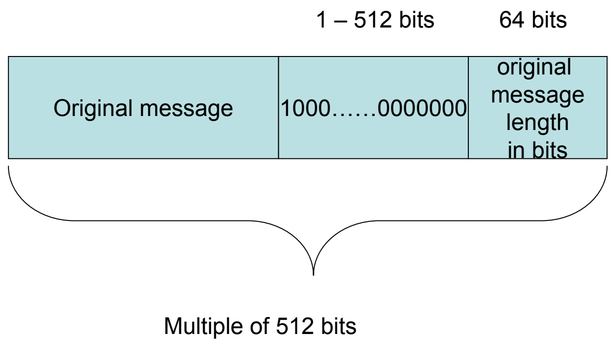
MD2	RFC 1319	128 bit
MD4	RFC 1320	128 bit
MD5	RFC 1321	128 bit
SHA-1	NIST	160 bit

SHA-1 Overview

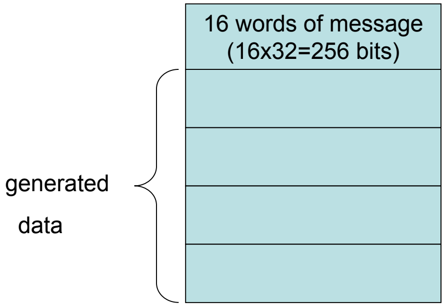


post stage MD = pre stage MD + 160 bit result of compression

SHA-1 Padding



SHA-1 Stage Operation (I)



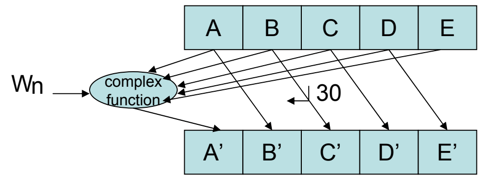
512 bit message block has 16 32bit words $W_0\ W_1, W_2, \ldots W_{15}$

For $n \geq 16$,

$W_n = W_{n-3} \oplus W_{n-8} \oplus W_{n-14} \oplus W_{n-16}$

where $\oplus$ is bitwise exclusive or

SHA-1 Stage Operation (II)



For n = 0,1,2,…79
$A' = E + (A \lll 5) + W_n + K_n + f(n,B,C,D)$

where $\lll 5$ is left rotate 5 bits, and the "constant" K_n takes different values for the ranges (0-19), (20-39), (40-59), (60-79), and the function f() also depends on the same four ranges

The 80 iterations (n = 0, 1, 2,..79) is equivalent to 5 passes over a 16 x 32 = 512 bit message block

HMAC

- provides a standard way to compute a MAC using a hash function
- is a function of message and secret key
- is secure is underlying hash function is secure
- may be used with SHA-1 to give a 160 bit MAC

HMAC Overview