SECURE HASH ALGORITHM 1

Presented by
16IT133 – Ritvik Arya
16IT138 – Shreyas Shankar
16IT148 – Siddhant Waghjale
16IT232 – Nihar Chitnis

Secure Hash Algorithm (SHA)

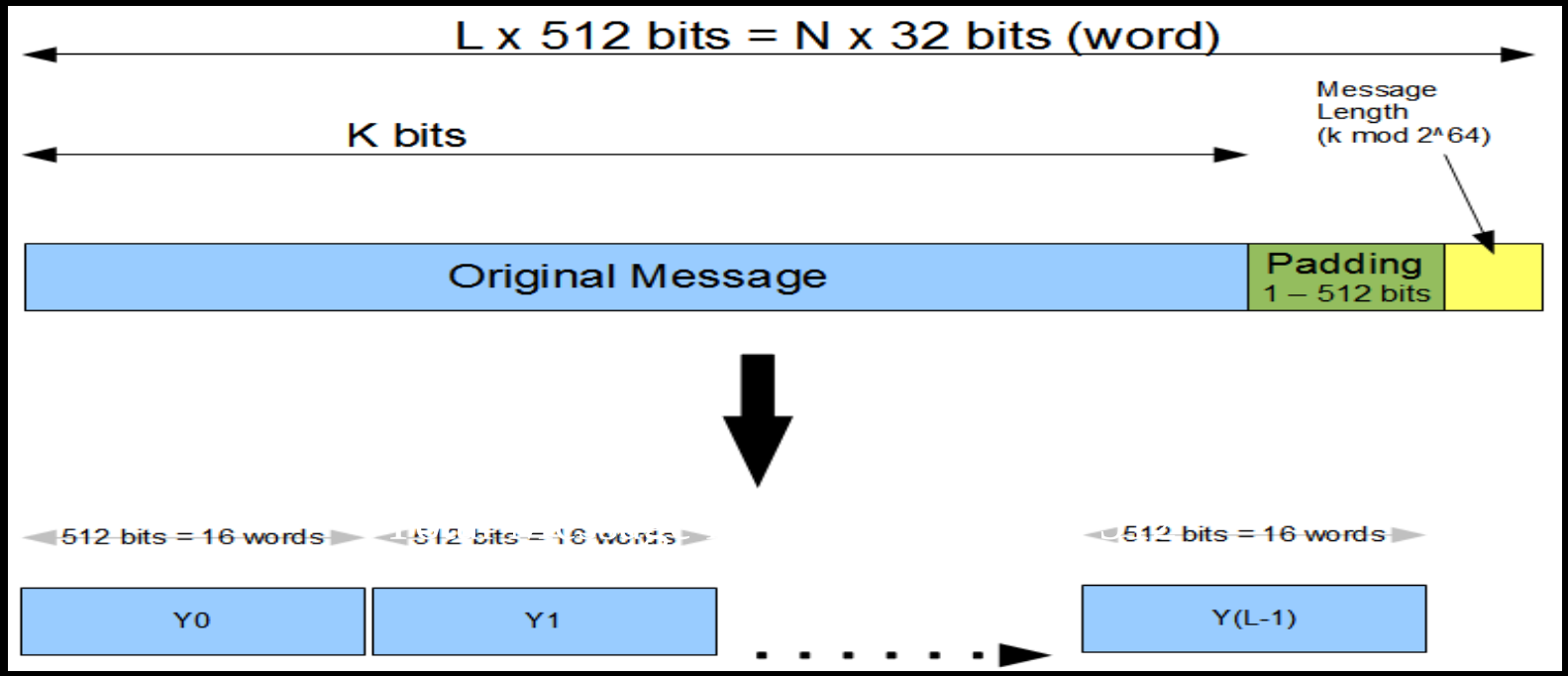
- Secure Hash Algorithm (SHA) was developed by NIST along with NSA.
- In 1993, SHA was published as a Federal Information Processing Standard.
- It has following versions-
  - SHA-0
  - SHA-1
  - SHA-2
  - SHA-3

SHA-1

- It works for any input message that is less than 2^{64} bits.
- The output of SHA is a message digest of 160 bits in length.
- This is designed to be computationally infeasible to:
  a) Obtain the original message , given its message digest.
  b) Find two messages producing the same message digest.

How SHA-1 works?

- *Step 1: Padding of Bits*



- *Step 2: Append Length*
- *Step 3: Divide the input into 512-bit blocks*

How SHA-1 works cont…

- *Step 4: Initialize chaining variables*

Chaining Variables	Hex values
A	01 23 45 67
B	89 AB CD EF
C	FE DC BA 98
D	76 54 32 10
E	C3 D2 E1 F0

- *Step 5: Process Blocks-* Now the actual algorithm begins….

How SHA-1 works cont…

- *Step 5.1 :* Copy chaining variables A-E into variables a-e.
- *Step 5.2 :* Divide current 512-bit block into 16 sub-blocks of 32-bits.
- *Step 5.3 :* SHA has 4 rounds, each consisting of 20 steps. Each round takes 3 inputs-
  - 512-bit block,
  - The register abcde
  - A constant K[t] (where t= 0 to 79)

Round	Value of t between
1	1 and 19
2	20 and 39
3	40 and 59
4	60 and 79

How SHA-1 works cont…

- *Step 5.4 :* SHA has a total of 80 iterations (4 rounds X 20 -iterations). Each iteration consists of following operations:-

$$abcde = (e + \text{Process P} + S^5(a) + W[t] + K[t]), a, S^{30}(b) , c , d$$

Where,

abcde = The register made up of 5 variables a, b, c, d, e.

Process P = The logic operation.

S^t = Circular-left shift of 32-bit sub-block by t bits.

W[t[= A 32-bit derived from the current 32-bit sub-block.

K[t] = One of the five additive constants.

How SHA-1 works cont…

- *Process P in each SHA round*

Round	Process P
1	(b AND c) OR ((NOT b) AND (d))
2	b XOR c XOR d
3	(b AND c) OR (b AND d) OR (c AND d)
4	b XOR c XOR d

How SHA-1 works cont…

- *The values of W[t] are calculated as follows :*
  - For the first 16 words of W (i.e. t=0 to 15) , the contents of the input message sub-block M[t] become the contents of W[t].
  - For the remaining 64 values of W are derived using the equation

$$W[t] = s^1 (W[t-16] \text{ XOR } W[t-14] \text{ XOR } W[t-8] \text{ XOR } W[t-3])$$

Comparison between MD5 and SHA-1

Point of discussion	MD5	SHA-1
Message digest length in bits	128	160
Attack to try and find the original message given a message digest	Requires 2^{128} operations to break in.	Requires 2^{160} operations to break in, therefore more secure.
Attack to try and find two messages producing same message digest	Requires 2^{64} operations to break in.	Requires 2^{80} operations to break in.
Speed	Faster	Slower
Successful attempts so far	There have been reported attempts to some extent.	No such claims so far.

Conclusion

- Developing Secure Hash Algorithm was initially major concern for defense authorities.
- SHA produces message digest which has an application in digital signature.
- In this way, this technique took a contributed in secure and robust encryption.