Sanjivani Rural Education Society's

Sanjivani College of Engineering, Kopargaon-423603

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

NAAC 'A' Grade Accredited, ISO 9001:2015 Certified

Department of Information Technology

(NBA Accredited)

Cryptography and Cyber Security [IT311]

Mrs. Kanchan D. Patil

Assistant Professor

Unit 3: Message Digest & Key Management

- Hash Algorithms: SHA-1, MD5, Key Management: Introduction, Key Management: Generations, Distribution, Updation, Digital Certificate, Digital Signature, Kerberos 5.0.

Secure Hash Algorithm (SHA)

- Secure Hash Algorithms (SHA) was developed by National Institute of Standards and Technology (NIST) along with NSA
- Published as a Federal Information Processing Standards Publications (FIPS 180 PUBS) in 1993
- A revised version was issued as FIPS PUB 180-1 in 1995 and is referred to as SHA-1
- SHA is a modified version of MD5
- Name of Standard: Secure Hash Signature Standard (SHS)
- In 2002 , NIST produced a revised version of the standard, FIPS 180-2 that defined three new versions of SHA as SHA-256, SHA-384, and SHA-512.

Secure Hash Algorithm (SHA) : Purpose

- Purpose of SHA is authentication and not the encryption
- Verify that received messages come from the alleged source and have not been altered.
- Verify the sequence and timing.
- Digital Signature is used to combat denial of receipt of a message by either the source or destination.
- Impossible to recreate a message given a message digest.

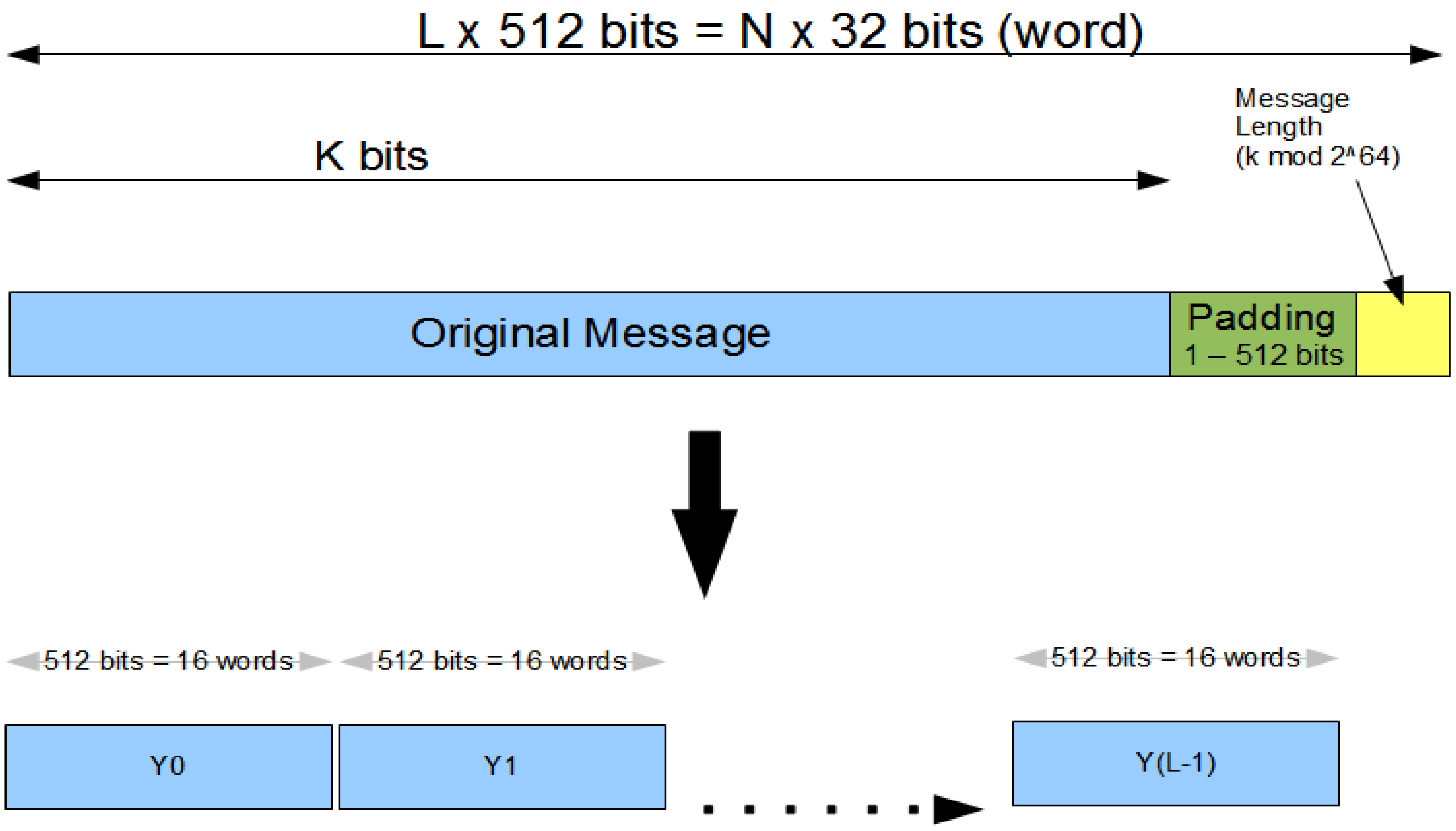
Secure Hash Algorithm (SHA) : Applications

- SHA uses one way hash function. The applications are as follows:
- Public Key Algorithms
  - Password Logins
  - Encryption Key Management
  - Digital Signatures
- Integrity Checking
  - Virus and Malware Scanning
- Authentication
  - Secure Web Connections (PGP, SSL, SSH, S/MIME)

Secure Hash Algorithm (SHA) : Variants

- MD4 and MD5 by Ron Rivest (1990,1994)
- SHA-0, SHA-1 by NSA (1993, 1995)
- RIPEMD-160 (1996)
- SHA-2 (2002 – 224, 256, 385, 512)
- Whirlpool
- Tiger
- GOST-3411
- SHA-3
    - Winner selected from solicitations in 2012

Structure of SHA



Working of SHA

- SHA is closely modeled after MD5

- **Step 1: Padding**
  - To add padding to the end of the original message in such a way that the length of the message is **64 bits short of a multiple of 512**.
  - Like MD5, the padding always added, even if the message is already 64 bits short of a multiple of 512.

Working of SHA

- **Step 2: Append length**
  - The length of the message excluding the length of the padding is calculated and appended to the end of the padding as a 64-bit block.

- **Step 3: Divide the input into 512-bit blocks**
  - The input message is now divided into blocks, of length 512 bits.
  - These blocks become the input to the message digest processing logic.

Working of SHA

- **Step 4: Initialize chaining variables**
  - Five chaining variables A through E
  - In the case of SHA want to produce a message digest of length 160 bits, we need to have **five chaining variables** here (5 x 32 = 160 bits).
  - In SHA, the variables A through D have the same values as they had in MD5

A	Hex	01	23	45	67
B	Hex	89	AB	CD	EF
C	Hex	FE	DC	BA	98
D	Hex	76	54	32	10

  - Additionally, **E is initialized to Hex C3 D2 E1 F0.**

Working of SHA

- **Step 5: Process Blocks**
  - **Step 5.1:**
    - Copy the chaining variables A-E into variables a-e.
    - The combination of a-e, called as **abede** will be considered as a **single register** for storing the temporary intermediate as well as the final results.
  - **Step 5.2:**
    - Now, divide the current 512-bit block into 16 sub-blocks, each consisting of 32 bits.

Working of SHA

- **Step 5: Process Blocks**
  - **Step 5.3:** SHA has four rounds, each round consisting of 20 steps.
    - Each round takes three inputs
      - Current 512- bit block
      - Register abcde
      - A constant K[t] (where t=0 to 79)
    - It then updates the contents of the register abcde using the SHA algorithm steps.
    - We have only four constants (in case of MD5-64 constants) defined for K[t], one used in each of the four rounds.

Working of SHA

- **Step 5: Process Blocks**
  - **Step 5.3:** We have only four constants (in case of MD5- 64 constants) defined for K[t], one used in each of the four rounds.

Round	*Value of t between*	*K[t] in hexadecimal*	*K[t] in decimal (Only integer portion of the value shown)*
1	1 and 19	5A 92 79 99	$2^{30} \times \sqrt{2}$
2	20 and 39	6E D9 EB A1	$2^{30} \times \sqrt{3}$
3	40 and 59	9F 1B BC DC	$2^{30} \times \sqrt{5}$
4	60 and 79	CA 62 C1 D6	$2^{30} \times \sqrt{10}$

Working of SHA

- **Step 5.4**
  - SHA consists of four rounds, each round containing 20 iterations.
  - This makes it a total of 80 iterations.
  - Mathematically, an iteration consists of the following operations:

    abcde = (e + Process P+s^5(a)+ W[t] + K[t]), a, s^30 (b), c,d

Where,

abcde = The register made up of the five variables a, b, c, d and e

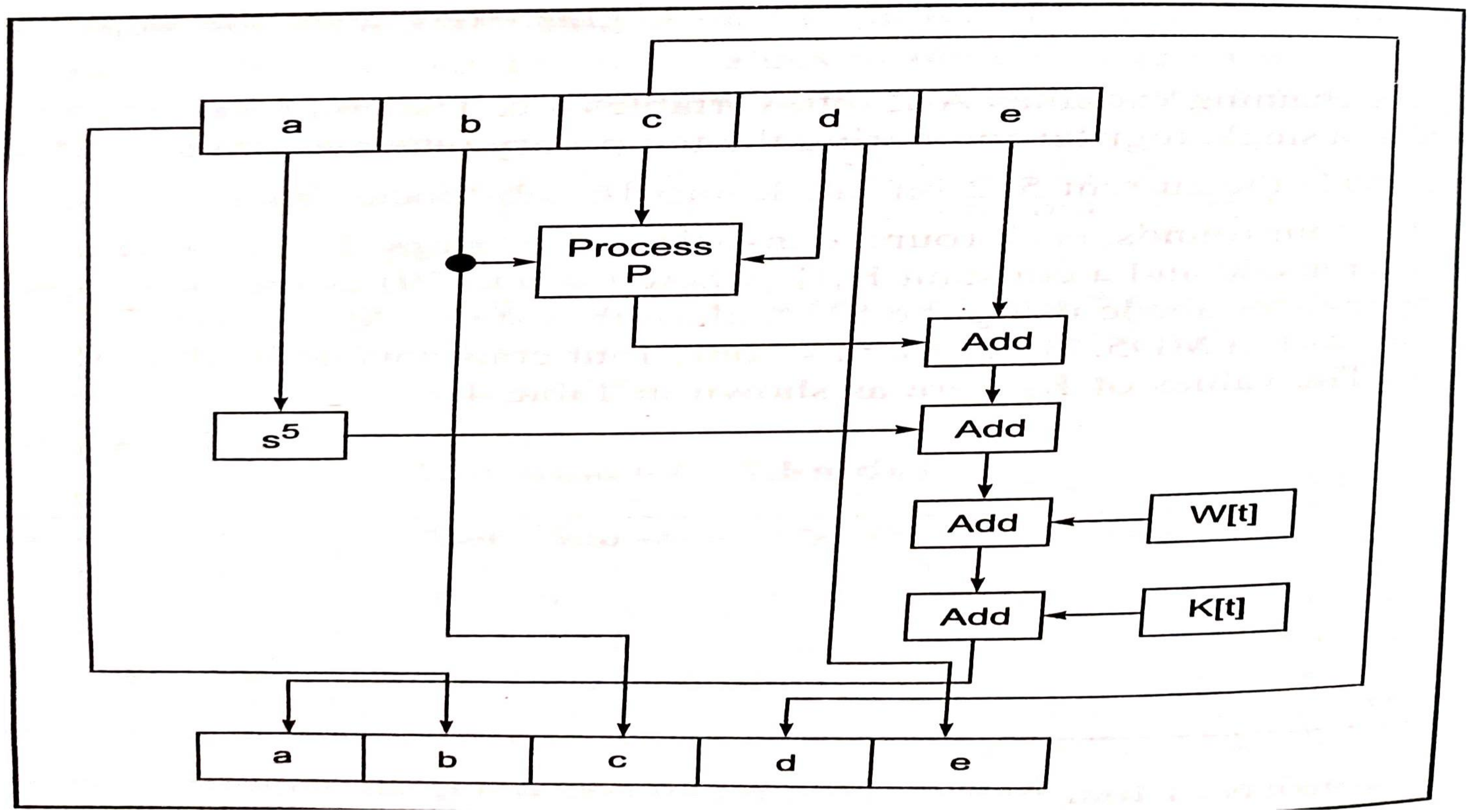
Process P = The logical operation

S^t = Circular-left shift of the 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

Working of SHA : Single SHA-1 Iteration



Working of SHA

- **Step 5.4** : Process P in each SHA-1 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

Working of SHA

- **Step 5.4**
  - The values of W[t] can be calculated as follows:
  - For the first 16 words of W (ie. t = 0 to 15), the contents of the input message sub-block M[t] become the contents of W[t] straightaway.
  - That is, the first 16 blocks of the input message M copied to W.
  - The remaining 64 values of W are derived using the equation:

W[t] = s' (W[t-16] XOR W[t-14] XOR W[t-8] XOR W[t-3])

s' indicates a circular-left shift (i.e. rotation) by 1 bit position.

Cryptanalysis and Limitation

- Key Premises for Hash Functions:
  - Impossible to re-create a message given a fingerprint
  - Collision Free

- SHA-1 failure using brute force attack in 2^{80} operations

Comparison of SHA Parameters

	SHA-1	SHA-256	SHA-384	SHA-512
Message digest size	160	256	384	512
Message size	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block size	512	512	1024	1024
Word size	32	32	64	64
Number of steps	80	64	80	80
Security	80	128	192	256

Notes: 1. All sizes are measured in bits.
2. Security refers to the fact that a birthday attack on a message digest of size n produces a collision with a workfactor of approximately $2^{n/2}$.

Difference Between MD5 and SHA-1

Sr. No.	Points of Discussion	MD5	SHA-1
1	Message digest length in bits	128	160
2	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. more secure
3	Attack to try and find two messages producing the same message digest	Requires 2^64 operations to break in	Requires 2^80 operations to break in
4	Successful attacks so far	Attempts reported so far	No reported yet
5	Speed	Faster (64 iterations and 128-bit buffer)	Slower (80 iterations and 160-bit buffer)
6	Software implementation	Simple. Does not need any large programs or complex tables	Simple. Does not need any large programs or complex tables

References:

- Atul Kahate,"Cryptography and Network Security", second edition, Tata McGraw Hill
- William Stallings, "Cryptography and Network Security-Principles and practice"