Cryptography and Network Security

MD5

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	24 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

Birthday Attacks

- might think a 64-bit hash is secure
- but by **Birthday Paradox** is not
- **birthday attack** works thus:
  - opponent generates $2^{m/2}$ variations of a valid message all with essentially the same meaning
  - opponent also generates $2^{m/2}$ variations of a desired fraudulent message
  - two sets of messages are compared to find pair with same hash (probability > 0.5 by birthday paradox)
  - have user sign the valid message, then substitute the forgery which will have a valid signature
- conclusion is that need to use larger MACs

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

Hash Function Properties

- a Hash Function produces a fingerprint of some file/message/data

  `h = H(M)`

  – condenses a variable-length message M

  – to a fixed-sized fingerprint

- assumed to be public

Block Ciphers as Hash Functions

- can use block ciphers as hash functions
  - using H_0=0 and zero-pad of final block
  - compute: $H_i = E_{M_i} [H_{i-1}]$
  - and use final block as the hash value
  - similar to CBC but without a key
- resulting hash is too small (64-bit)
  - both due to direct birthday attack
  - and to “meet-in-the-middle” attack
- other variants also susceptible to attack

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

Hash Algorithms

- similarities in the evolution of hash functions & block ciphers
  - increasing power of brute-force attacks
  - leading to evolution in algorithms
  - from DES to AES in block ciphers
  - from MD4 & MD5 to SHA-1 & RIPEMD-160 in hash algorithms
- likewise tend to use common iterative structure as do block ciphers

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

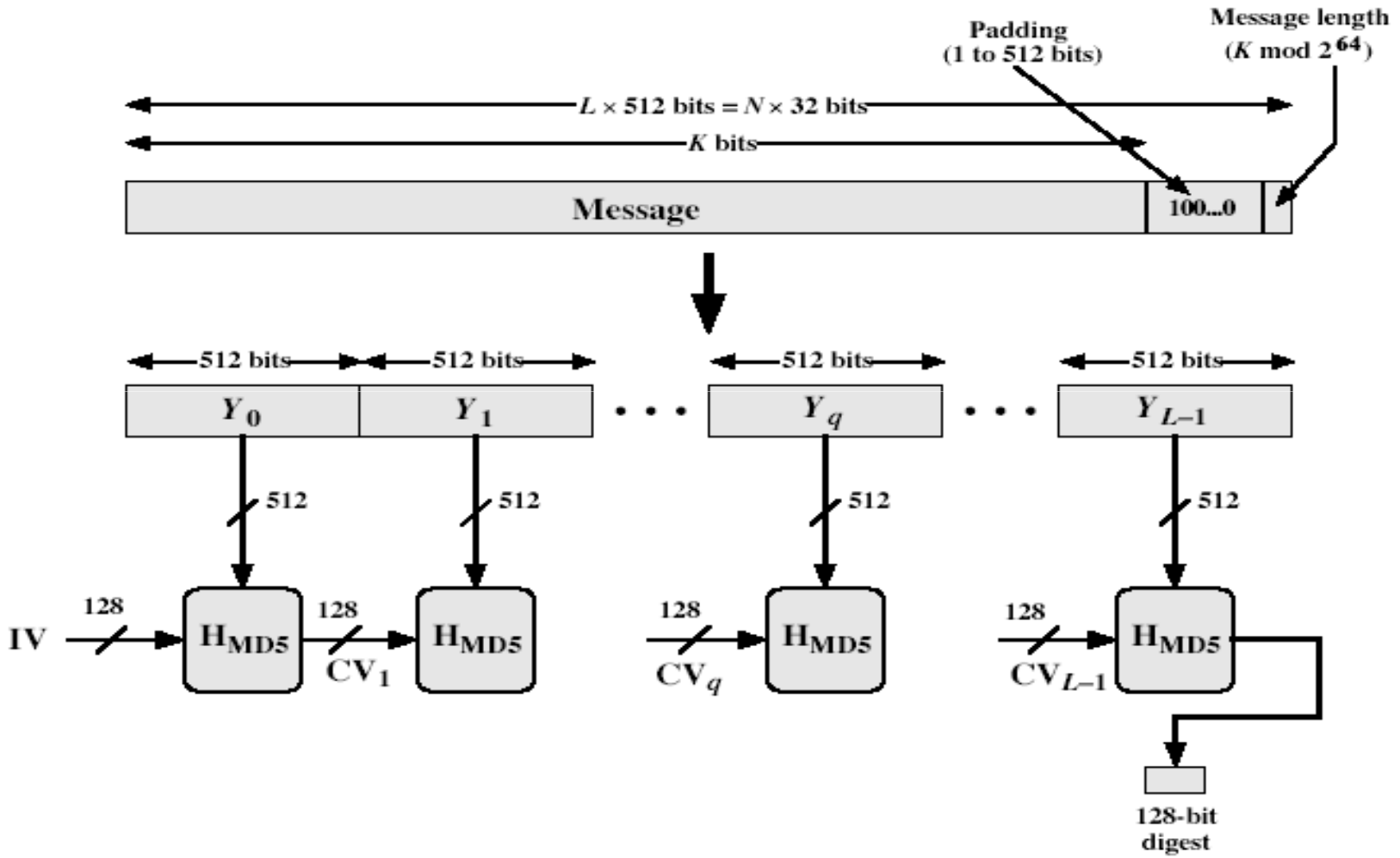
MD5

- designed by *Ronald Rivest* (the "*R*" in RSA)
- latest in a series of MD2, MD4
- produces a 128-bit hash value
- until recently was the most widely used hash algorithm
  - in recent times have both brute-force & cryptanalytic concerns
- specified as Internet standard RFC1321

MD5 Overview

1. pad message so its length is 448 mod 512
2. append a 64-bit length value to message
3. initialise 4-word (128-bit) MD buffer (A,B,C,D)
4. process message in 16-word (512-bit) blocks:
   - using 4 rounds of 16 bit operations on message block & buffer
   - add output to buffer input to form new buffer value
5. output hash value is the final buffer value

MD5 Overview



MD5 Compression Function

- each round has 16 steps of the form:

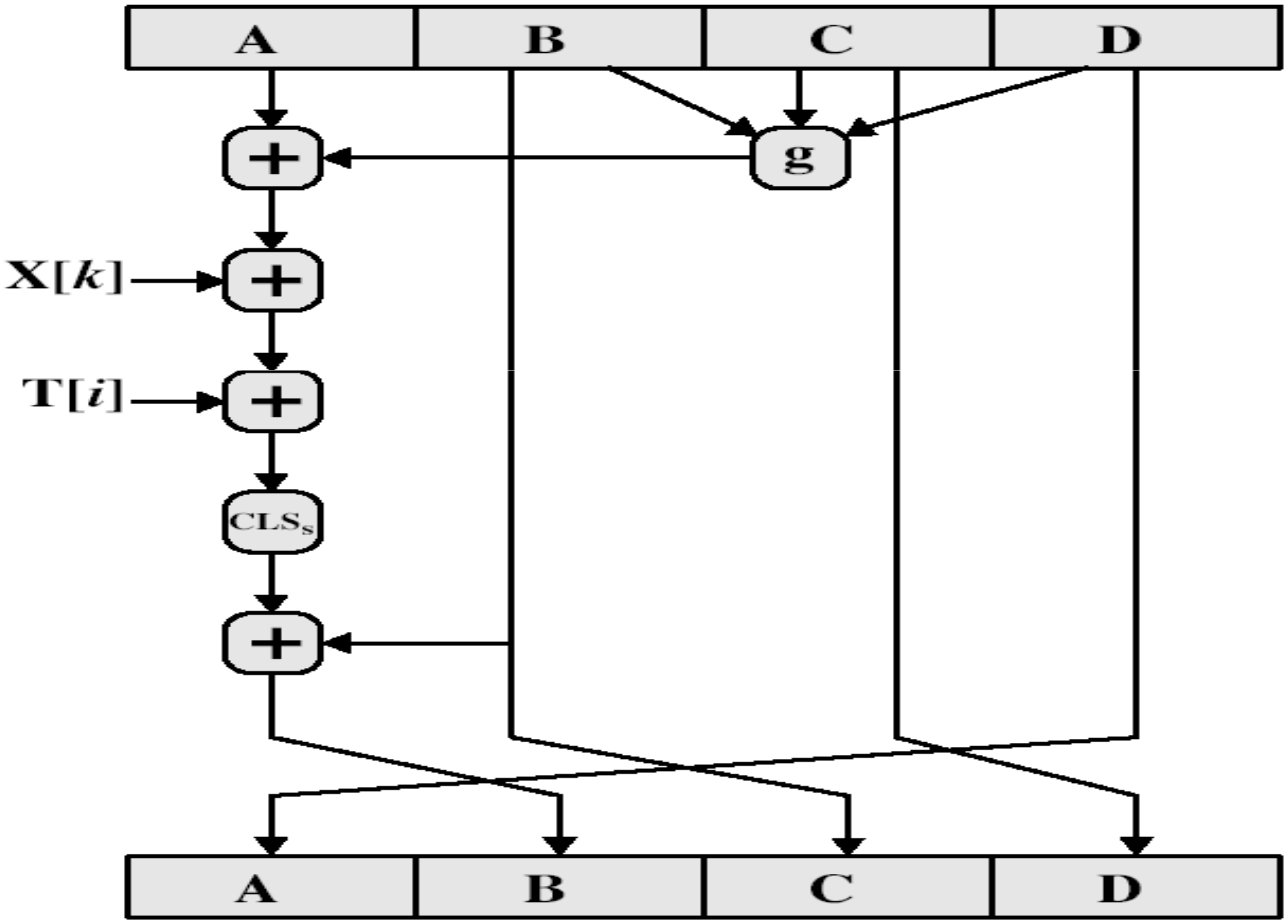
```
a = b+((a+g(b,c,d)+X[k]+T[i])<<<s)
```

- a,b,c,d refer to the 4 words of the buffer, but used in varying permutations
  - note this updates 1 word only of the buffer
  - after 16 steps each word is updated 4 times
- where g(b,c,d) is a different nonlinear function in each round (F,G,H,I)
- T[i] is a constant value derived from sin

MD5 Compression Function

- Each round mixes the buffer input with the next "word" of the message in a complex, non-linear manner.
- A different non-linear function is used in each of the 4 rounds (but the same function for all 16 steps in a round).
- The 4 buffer words (a,b,c,d) are rotated from step to step so all are used and updated.
- g is one of the primitive functions F,G,H,I for the 4 rounds respectively.
- X[k] is the kth 32-bit word in the current message block.
- T[i] is the ith entry in the matrix of constants T.
- The addition of varying constants T and the use of different shifts helps ensure it is extremely difficult to compute collisions.

MD5 Compression Function



Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

MD4

- precursor to MD5
- also produces a 128-bit hash of message
- has 3 rounds of 16 steps versus 4 in MD5
- design goals:
  - collision resistant (hard to find collisions)
  - direct security (no dependence on "hard" problems)
  - fast, simple, compact
  - favors little-endian systems (eg PCs)

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

Strength of MD5

- MD5 hash is dependent on all message bits
- Rivest claims security is good as can be
- known attacks are:
  - Berson 92 attacked any 1 round using differential cryptanalysis (but can't extend)
  - Boer & Bosselaers 93 found a pseudo collision (again unable to extend)
  - Dobbertin 96 created collisions on MD compression function (but initial constants prevent exploit)
- conclusion is that MD5 looks vulnerable soon

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

Summary

- have discussed:
  - digital signatures
  - ElGamal & Schnorr signature schemes
  - digital signature algorithm and standard

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

Test your understanding

1) What is birthday attack?
2) State the strength of MD5.
3) Explain in detail MD5.

Agenda

- Birthday attack
- Hash function properties
- Hash algorithm
- MD5
- MD4
- Strength of MD5
- Summary
- Test your understanding
- References

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.