A Presentation on – Improvements in MD5 security

based on the research paper-
“A Novel Improvement with an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document"
by Dr Ammar Mohammed Ali & Dr Alaa Kadhim Farhan”

BY:

MOHAMMED SHAHZAD

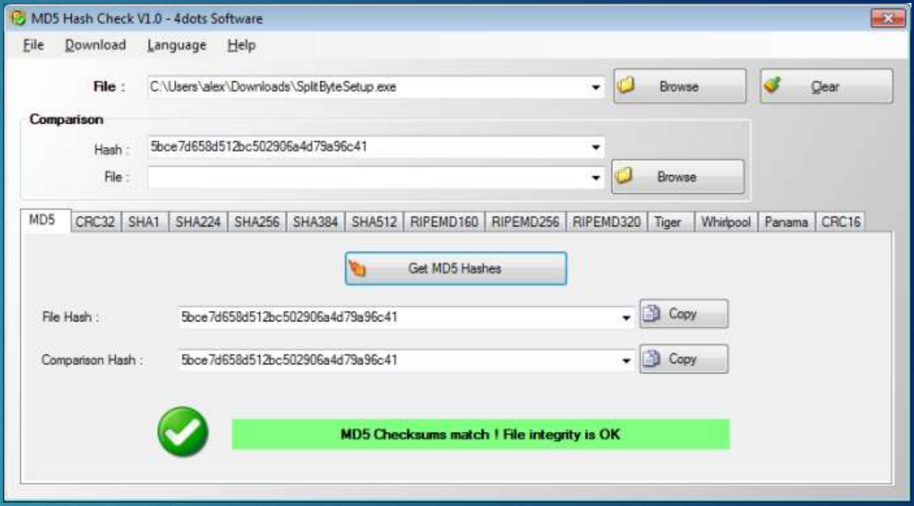
444105788@STUDENT.KSU.EDU.SA

Contents of this presentation

- Introduction to MD5 Hash function
  - The standard MD5 hash Function
  - Weaknesses
- The research – Improvements to existing MD5
  - The five suggested techniques
- Conclusion

Introduction to MD5 hash function

- Standard MD5 hash function
- The message-digest algorithm (MD5) as one-way cryptographic hash functions generally provides a 128-bit hash value.
- MD5 was designed by Ronald Rivest in 1991 to replace a more immediate hash function MD4.
- Most users are familiar with validating electronic documents based on a Hash function, to demonstrate the file/data integrity.
- Digital Signature after hashing



File : C:\Users\alex\Downloads\SplitByteSetup.exe

Comparison

Hash : 5bce7d658d512bc502906a4d79a96c41

File :

File Hash : 5bce7d658d512bc502906a4d79a96c41

Comparison Hash : 5bce7d658d512bc502906a4d79a96c41

MD5 Checksums match ! File integrity is OK

Checking file integrity with MD5

Introduction to MD5 hash function

- Standard MD5 hashing function
- A hash function H accepts a variable-length data M as input and produces a fixed-size hash value h
  - h = H(M)
  - Principal object is data integrity.
  - A change to any bit or bits in M results, in a major change to the hash code

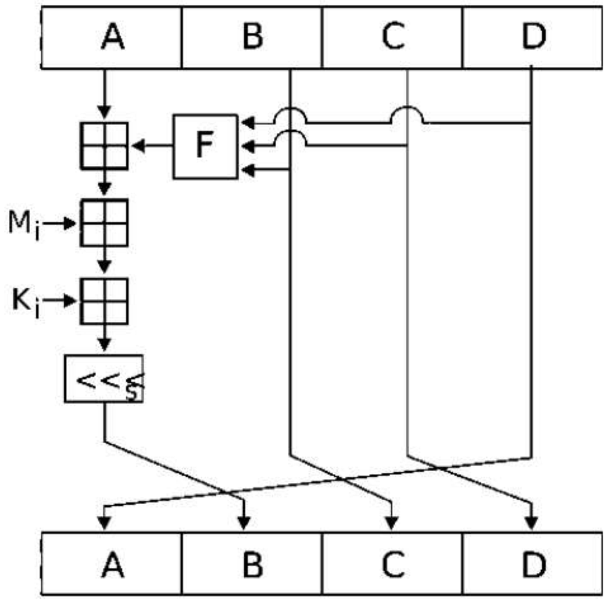


FIGURE 1. The block diagram of the main structure of existing MD5 schema.

Introduction to MD5 hash function

- Weaknesses In MD5 – potential attacks

- Researchers claim that existing MD5 is vulnerable to various attacks, including attacks with brute force, rainbow table, dictionary, Christmas, etc.
- The research focuses on eliminating the weaknesses that are inherent in the current MD5 algorithm, thereby ensuring data integrity and security.
- Stronger MD6 exists but not widely used.

Introduction to MD5 hash function

- Standard MD5 hash function in 5 steps
- 1. Appending the padding bits as preprocess. The resulting message length is a multiple of 512.
- 2. Append the length of message
- 3. Initialize MD buffer. Recorders are configured as a four-word buffer (A, B, C, and D) to calculate the message digest. Initialize variables: (A = 67452301, B = efcdab89, C = 98badcfe, D = 10325476).
- 4. Process the message It consists generally of four cycles; In each cycle, 16 steps are performed on the recorders for data confusion.
- 5. Output. After processing of all blocks, plain text is converted into ciphertext or hash form as a message digest, where the final value is 128 bits. This is called digest.

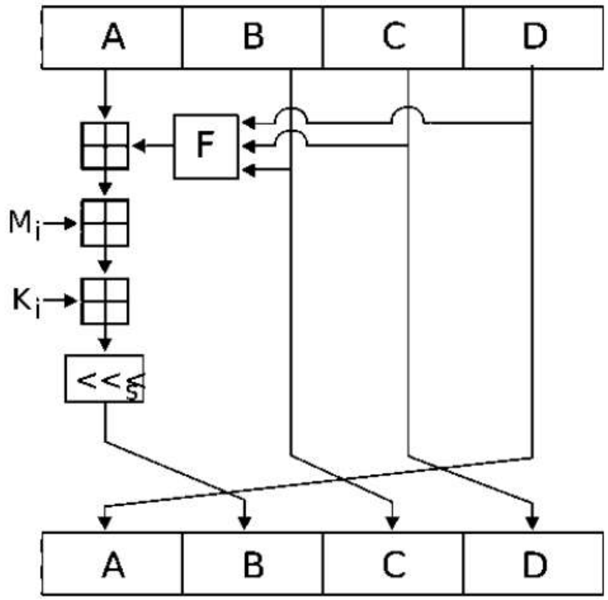


FIGURE 1. **The block diagram of the main structure of existing MD5 schema.**

The research

- Improvements suggested:
- The researchers recommend that more powerful security and elasticity can be achieved for the current MD5 128-bit algorithm by modifying length of the message digest.
- The researchers also propose the use of a key to eliminate threats that commonly appear in rainbow attacks and dictionary attacks.
- 5 Methods for more collision-resistant MD5.

The research

- Related reseach

- Research present an implemented hybrid cryptography that uses both MD5 and the proprieties of an elliptic curve cryptosystem (ECC) to generate key steam.
- Other strategies to enhance MD5 include, applying the concept of steganography combined with cryptography for increasing security.

The research

- Method 1: This method explores:

- The fusion of MD5 with **chaos theorem** (Fourth order Runge-kutta)
- **secret key**: The key length that is used in this method is the same as the plain text.
- The output hash length is variable (128-bit, 256-bit, 384-bit, 512-bit . . . etc).

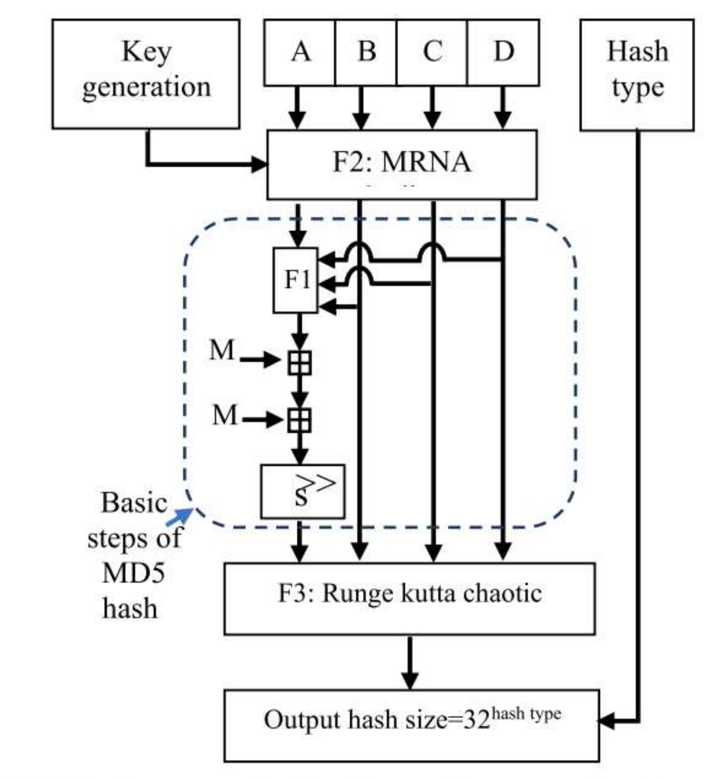


FIGURE 4. Show the general block diagram of the proposed system.

The research

- Method 2: this method explores:

- Basic MD5 with a secret key
- The length of key is the same as plain text length.
- The digest hash length has different lengths (128-bit, 256-bit, 384-bit,512-bit . . . etc).

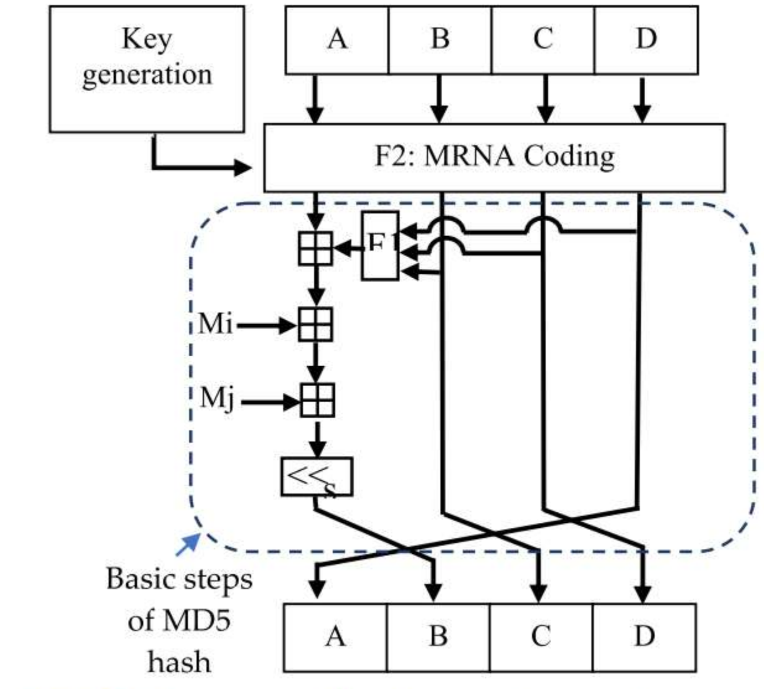


FIGURE 5. Shows the general block diagram of the proposed system (Method 2).

The research

- Method 3: This method:

- Basic steps of MD5 hash function with chaotic theorem only.
- No additional key is used
- The output hash length is variable (128-bit, 256-bit, 384-bit,512-bit . . . etc).

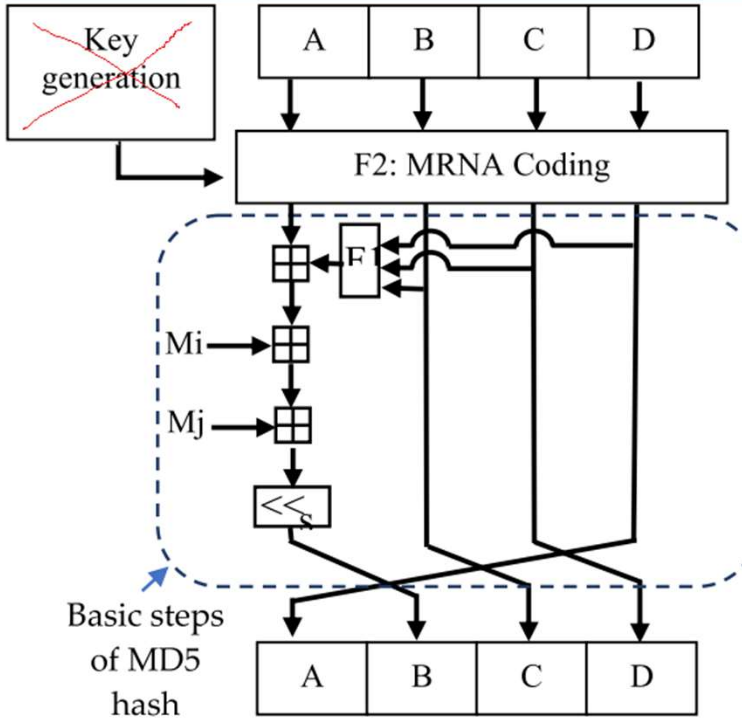


FIGURE 5. Shows the general block diagram of the proposed system (Method 2).

The research

- Method 4:

- Standard MD5 with
- length of key is fixed, predetermined by the user.
- The plain text is encrypted by performing a XOR with key.
- The output hash length is fixed(Either 128-bit, 256-bit, 384-bit,512-bit . . . etc).

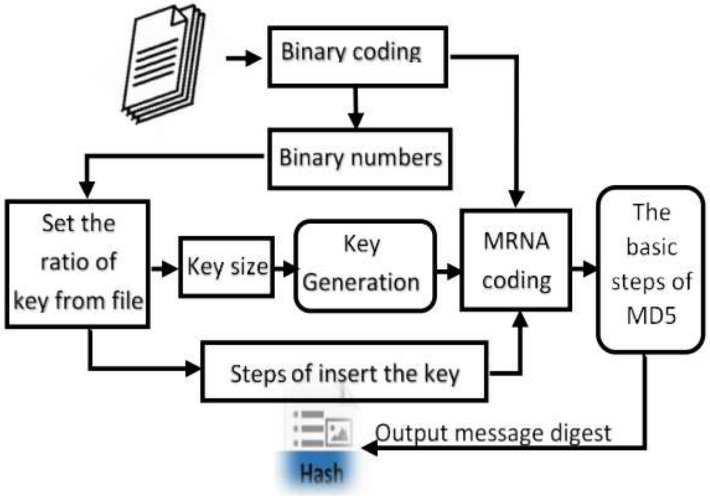


FIGURE 6. Shows the flow chart of general structure of the proposed system (Method 4).

The research

- Method 5:
- MD5 with chaos theorem & secret key.
- The output hash length is fixed(128-bit).

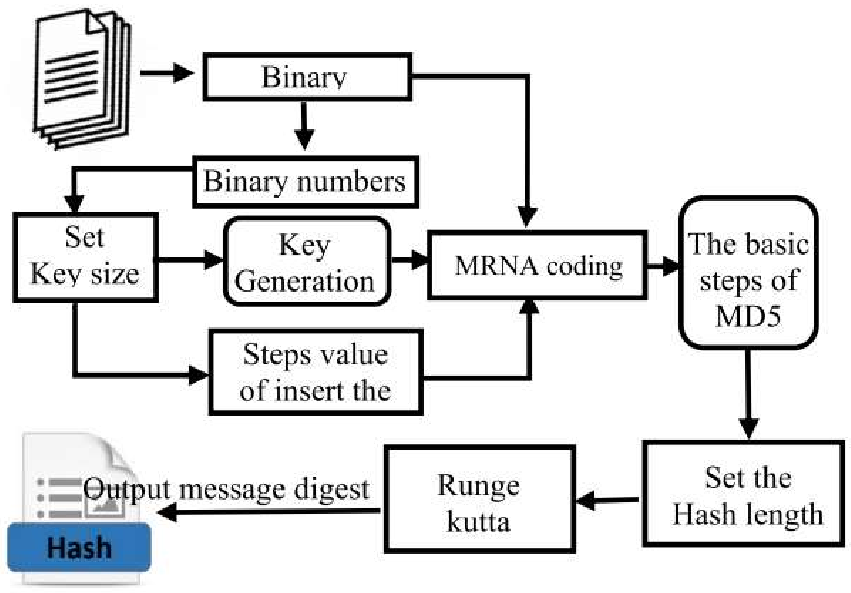


FIGURE 7. **Shows the flow chart of the proposed system method 5.**

Conclusion

- The length of the hash digest of the MD5 algorithm is often considered a weak point of the algorithm.
- Figure: Comparison of various methods.
- Based on their research findings, Method 2 is best

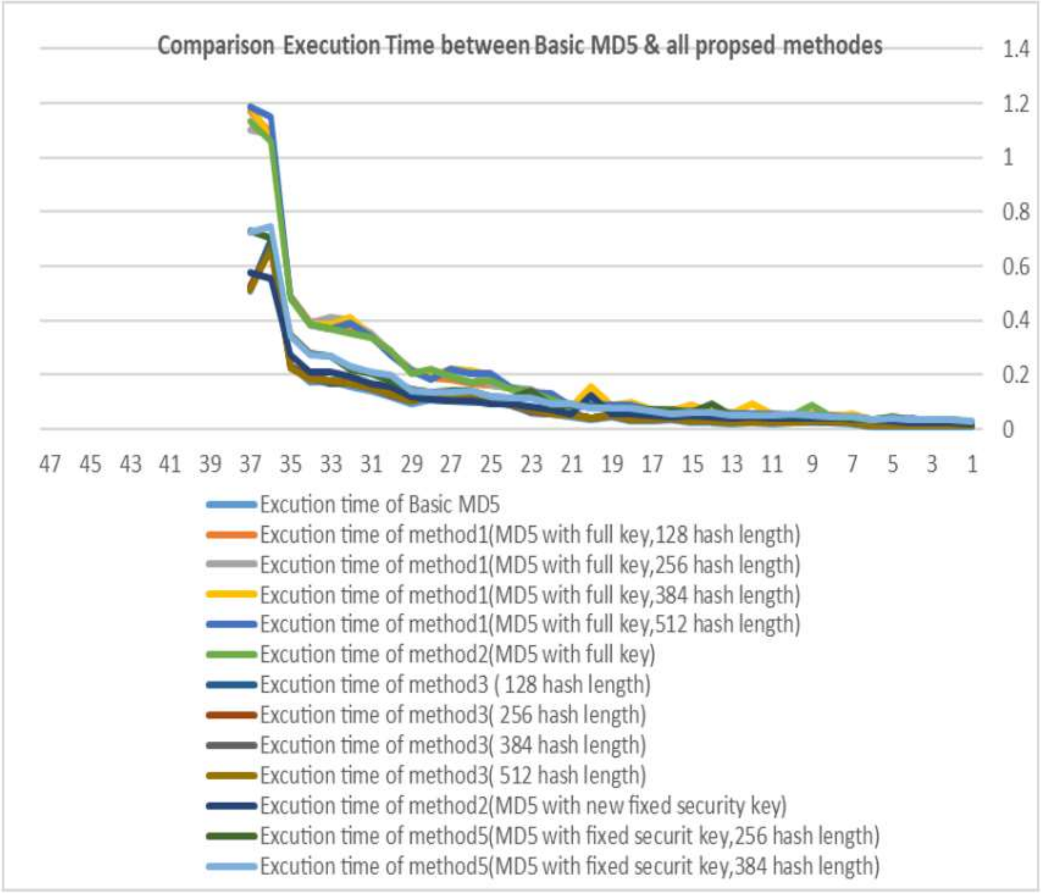


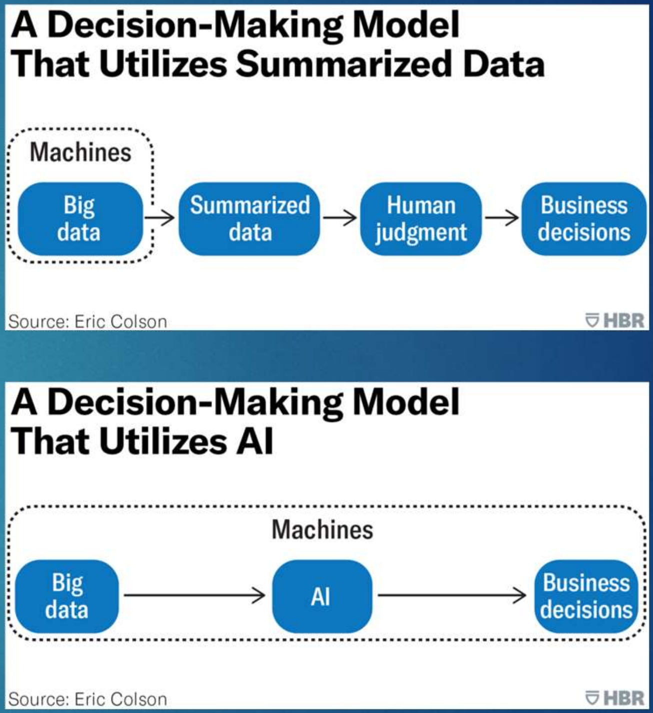
FIGURE 9. **Comparison of the run time between the multiple development methods with the actual way.**

Conclusion

- Overall, their work is an important asset to the MD5 research and the study of prospective improvements in MD5 hash function.
- They seem to have missed more important citations.
- The work was not proof-read for common grammatical and punctuation mistakes and has an unconventional flow of ideas and vocabulary, which make it difficult to follow for novice researchers and casual readers.
- Approach to the problem is realistic, main concept is explained very clearly. Results discussion and analysis are more than sufficient.
- The research work inspires further elaboration and research in improving existing hash functions.

Conclusion

- The improvement in the proposed MD5 algorithm will result in an improved collision resistance to maintain data integrity.
- Points to ponder
  - Hash functions affirm data integrity at data level.
  - Data integrity is crucial for everyone, from general file integrity to AI-driven decision making.



A Decision-Making Model That Utilizes Summarized Data

Source: Eric Colson

A Decision-Making Model That Utilizes AI

Source: Eric Colson

Data integrity for decision making

Thank You!