G.ENKRIPSI DATA

Berikut adalah penjelasan tentang beberapa metode enkripsi dan hashing yang kamu sebutkan 🔒:

1. MD2 (Message Digest Algorithm 2)

- *Tipe*: Fungsi hash kriptografi
- *Output*: 128-bit hash value
- *Karakteristik*: Dirancang untuk integritas data, sekarang dianggap tidak aman
- *Penggunaan*: Dahulu untuk checksum, jarang digunakan sekarang

2. MD4 (Message Digest Algorithm 4)

- *Tipe*: Fungsi hash
- *Output*: 128-bit hash
- *Karakteristik*: Predecessor MD5, ditemukan memiliki kelemahan keamanan
- *Status*: Tidak direkomendasikan untuk penggunaan keamanan

3. MD5 (Message Digest Algorithm 5)

- *Tipe*: Fungsi hash kriptografi
- *Output*: 128-bit hash value
- *Karakteristik*: Luas digunakan tapi sekarang dianggap rawan terhadap collision attack
- *Penggunaan*: Dahulu untuk integritas data, checksum; tidak disarankan untuk keamanan kritis

4. SHA (Secure Hash Algorithm)

- *Tipe*: Fungsi hash kriptografi

- *Varian*: SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3
- *Karakteristik*: Dirancang untuk keamanan tinggi
- *Penggunaan*: SHA-256 dan SHA-3 dianggap aman untuk aplikasi kriptografi
- *Catatan*: SHA-1 sudah tidak dianggap aman

5. RC4 (Rivest Cipher 4)
- *Tipe*: Stream cipher
- *Karakteristik*: Algoritma enkripsi simetris, dulu populer untuk SSL/TLS
- *Keamanan*: Ditemukan memiliki kelemahan, tidak direkomendasikan untuk penggunaan baru
- *Penggunaan*: Dahulu digunakan di WEP, SSL/TLS (sekarang banyak digantikan)

6. Base64
- *Tipe*: Encoding, bukan enkripsi
- *Fungsi*: Mengubah data biner ke format teks ASCII untuk transmisi
- *Karakteristik*: Bukan metode enkripsi, digunakan untuk encoding data (misal email attachments)
- *Penggunaan*: Umum untuk encoding data di aplikasi seperti email, data URI

Perbedaan Utama
- *Hashing (MD5, SHA)*: satu arah, untuk integritas data, bukan enkripsi
- *Enkripsi (RC4)*: dua arah (enkripsi-dekripsi), untuk kerahasiaan
- *Encoding (Base64)*: bukan untuk keamanan, untuk representasi data

Catatan Keamanan

- Banyak algoritma lama (MD2, MD4, MD5, RC4) dianggap tidak aman untuk aplikasi keamanan modern
- SHA-2, SHA-3 umumnya dianggap lebih aman untuk hashing kriptografi

Kamu ingin tahu lebih tentang aplikasi hashing, enkripsi simetris/asimetris, atau penggunaan kriptografi dalam keamanan data?