HASH FUNCTION

H(M)=fixe length output(h)

F(my india)=(gshsjjmnsyssnjijngts) //fixed length output **called hash code/hash value/message digest**
F(22*2)=44

DEFINATION:
NON REVERSIBLE
FIX LENGTH OUTPUT
WEAK COLLISION/NO COLLISION

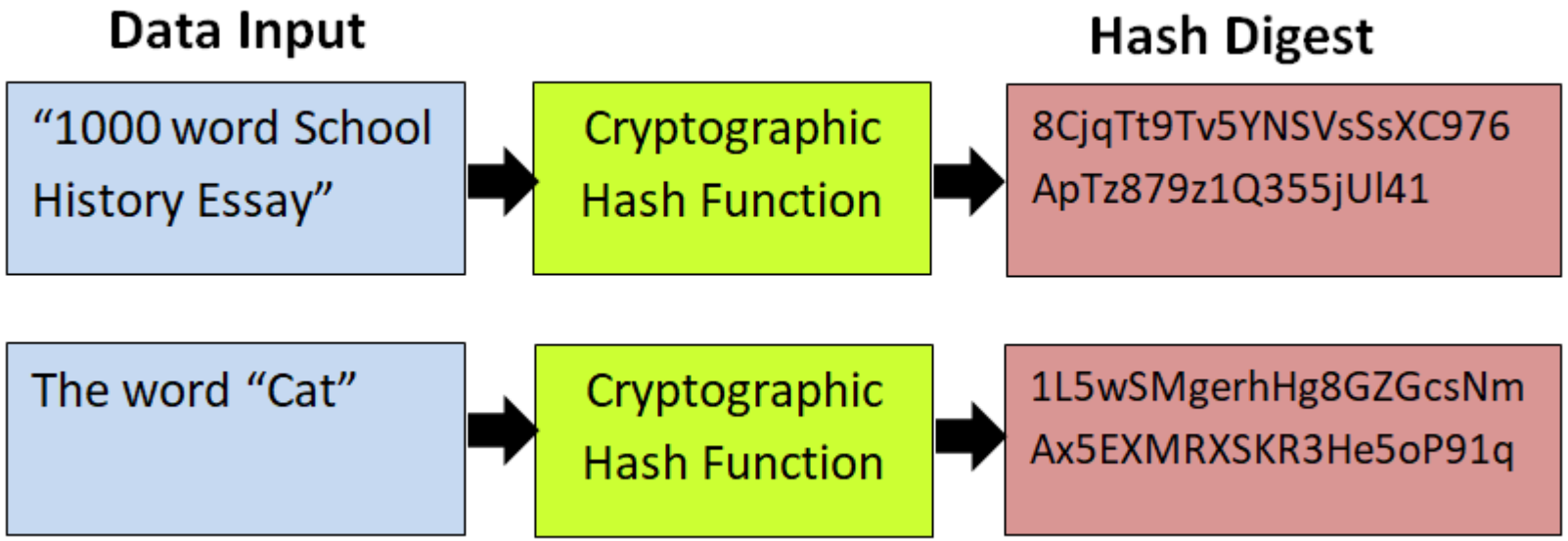
What Are Cryptographic Hash Functions?

A cryptographic hash function is a mathematical function used in cryptography. Typical hash functions take inputs of variable lengths to return outputs of a fixed length.

A cryptographic hash function combines the message-passing capabilities of hash functions with security properties.

NOTE:

- Hash functions are mathematical functions that transform or "map" a given set of data into a bit string of fixed size, also known as the "hash value."
- Hash functions are used in cryptography and have variable levels of complexity and difficulty.
- Hash functions are used for cryptocurrency, password security, and message security.

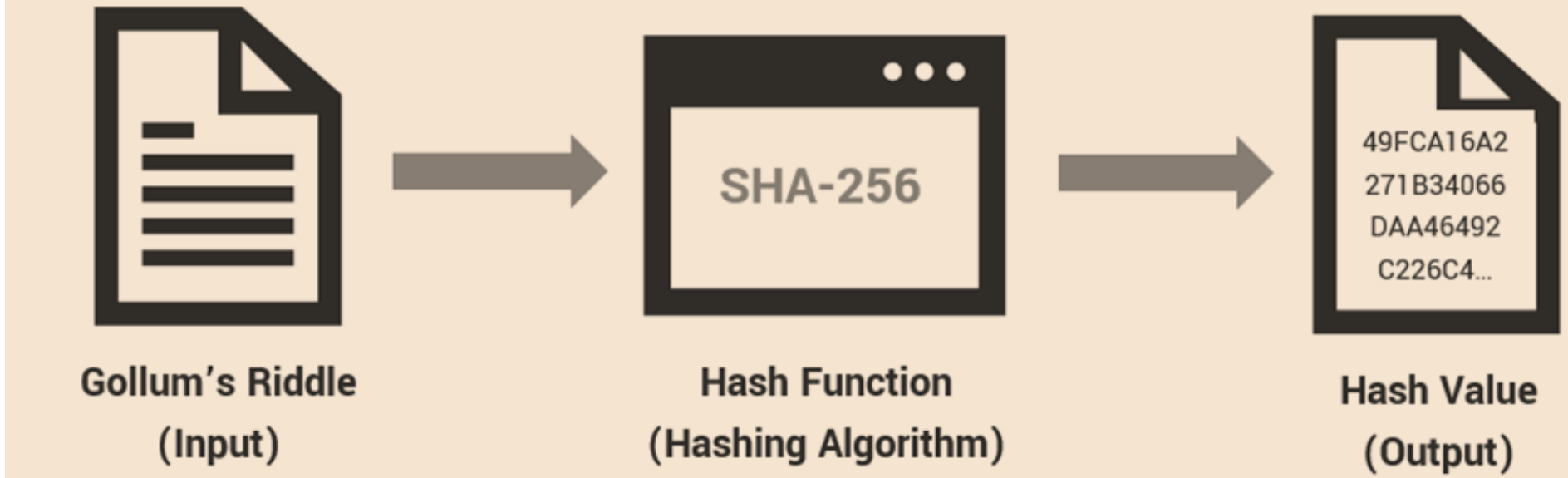


- Hash functions are extremely useful and appear in almost all information security applications.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.
- Values returned by a hash function are called **message digest** or simply **hash values**

What Does a Hash Function Do?

- Ensure data integrity,
- Secure against unauthorized modifications,
- Protect stored passwords, and
- Operate at different speeds to suit different purposes.

How Hashing Works



Examples of Common Hashing Algorithms & Families of Algorithms

- **Secure Hash Algorithm (SHA)** — This family of hashes contains SHA-1, SHA-2 (a family within a family that includes SHA-224, SHA-256, SHA-384, and SHA-512), and SHA-3 (SHA3-224, SHA3-256, SHA3-384, and SHA3-512). SHA-1 has been deprecated and the most commonly hashing algorithm now is SHA-256.

- **Message Digest (MD)** — This family of hashes contains a variety of hash functions that include MD2, MD4, MD5, and MD6. MD5 was long considered a go-to hashing algorithm but it's now considered broken because it results in collisions in the wild.

Applications of Cryptographic Hash Functions

Some of the uses of hashing include:

- Digital signatures,
- Biometrics,
- Password storage,
- Code signing certificates,
- Document signing certificates, and
- Email signing certificates.

When you have to compare a large piece of data or software, you can't check each code and word of it. But if you hash it, it converts big data into small, fixed-length hash values, which you can check and compare a lot more easily.