Sharif Ali BCS 7A
pro-0130

Date: Day:

Merkle damgard Construction:

Definition:
A method of building collision-resistant cryptographic hash functions from collision-resistant one-way compression functions.

Elaboration: The Merkle-Damgard Construction works by dividing the input message into blocks of fixed size, then processing them one at a time with the compression function. The output of each iteration is fed into next iteration, until the final block is processed. The output of the final iteration is the hash of the message.
The Merkle-Damgard construction is in many popular hash algorithms, such as MD5, SHA-1 and SHA-2.

Practical Examples: The merkle-Damgard construction is used to secure a wide variety of digital communications and trasactions. For example

1. Sign digital documents to ensure their authenticity and integrity.
2. protect passwords and other sensitive data from unauthorized access.
3. Verify the authenticity of software download.

p→o

Date: _____ Day: _____

(4) Secure financial transactions

Source Code

```
Class MerkleDamgardHash:
    def __init__(self, compression_function):
        self.compression_function = compression_function
        self.state = None

    def update(self, data):
        if self.state is None:
            self.state = self.compression_function(data)
        else:
            self.state = self.compression_function(self.state + data)

    def finalize(self):
        return self.state

def main():
    # Object
    hasher = MerkleDamgardHash(SHA256)
    # Update hash with "Hello, world!"
    hasher.update("Hello, world!")

    hash = hasher.finalize()

    # Print the hash
    print(hash.hex())

if __name__ == "__main__":
    main()
```

Scanned with CamScanner