School of Digital Media and Infocomm Technology

### ST2504 Applied Cryptography

1. Identify 4 main characteristics of a hash algorithm.

* **Fixed-length has value: arbitrary length of input, but always fixed-length of output**
* **No 2 identical digests if the message are different (collision resistant)**
* **It is irreversible (one-way function)**
* **Pseudo-randomness: digests from similar message must be very different**

2. Why is SHA-1 more secure than MD5?

* **Improved bit hashing which uses 80 iterations however much slower. Whereas, MD5 has 64 iterations.**
* **SHA-1 uses 160-bit hash value. Stronger against brute-force. (2160  operations to break)**
* **Introduction of more randomness.**

3. Contrast the two hash algorithm– SHA-1 and MD5.

|  |  |  |
| --- | --- | --- |
| **Characteristics** | **SHA1** | **MD5** |
| **Message digest length in bits** | 160 | 128 |
| **No. of Operations required to Brute force the algorithm** | 2160 operations | 2128 operations |
| **Internal construction of the function** | 80 iterations, and 160-bit buffers (5x32 bits word) | 64 iterations, with 128-bit buffers) |
| **Software implementation** | Simple, does not need any large programs or complex tables | Simple, does not need any large programs or complex tables |

4. What is Message Authentication Code (MAC)?

* **MAC is a one-way hash function.**
* **It requires both sender and recipient to know a shared(secret) key.**
* **It produces a hash value.**
* **To provide authentication for message.**
* **By using block cipher mode or hash function.**

5. What are the main differences between MAC and Hash?

* **MAC is a keyed hash function.**
* **MAC involves cryptographic processing to generate an authenticator.**
* **Hash is a keyless one-way hash function.**
* **Hash is a fingerprint of a message.**

6. What is the main application of a hash function?

**Public Key Algorithms:**

* **Password logins - Unix system**
* **Encryption Key Management**
* **Digital Signatures - RSA**

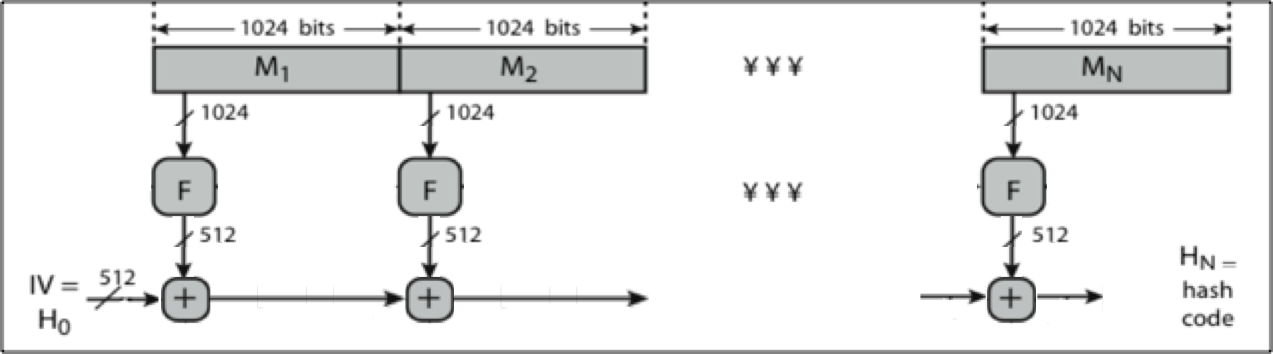
**Integrity Checking:**

* **Virus and malware scanning - signature**

**Authentication:**

* **Secure web connections - mutual authentication between client and server, i.e. SSL**

7. Given the following customed hashing algorithm, which uses SHA-2 as its core function [F], it is proven that 2 main hash characteristics 1) One Way Hash and 2) Collision Resistance can be compromised with suitable conditions such as adversary could get the hash digests of the same message with decreasing number of similar blocks.



Explain how the algorithm above could be improved.

**Use Merkle-Damgard construction as shown below (one more input to F)**