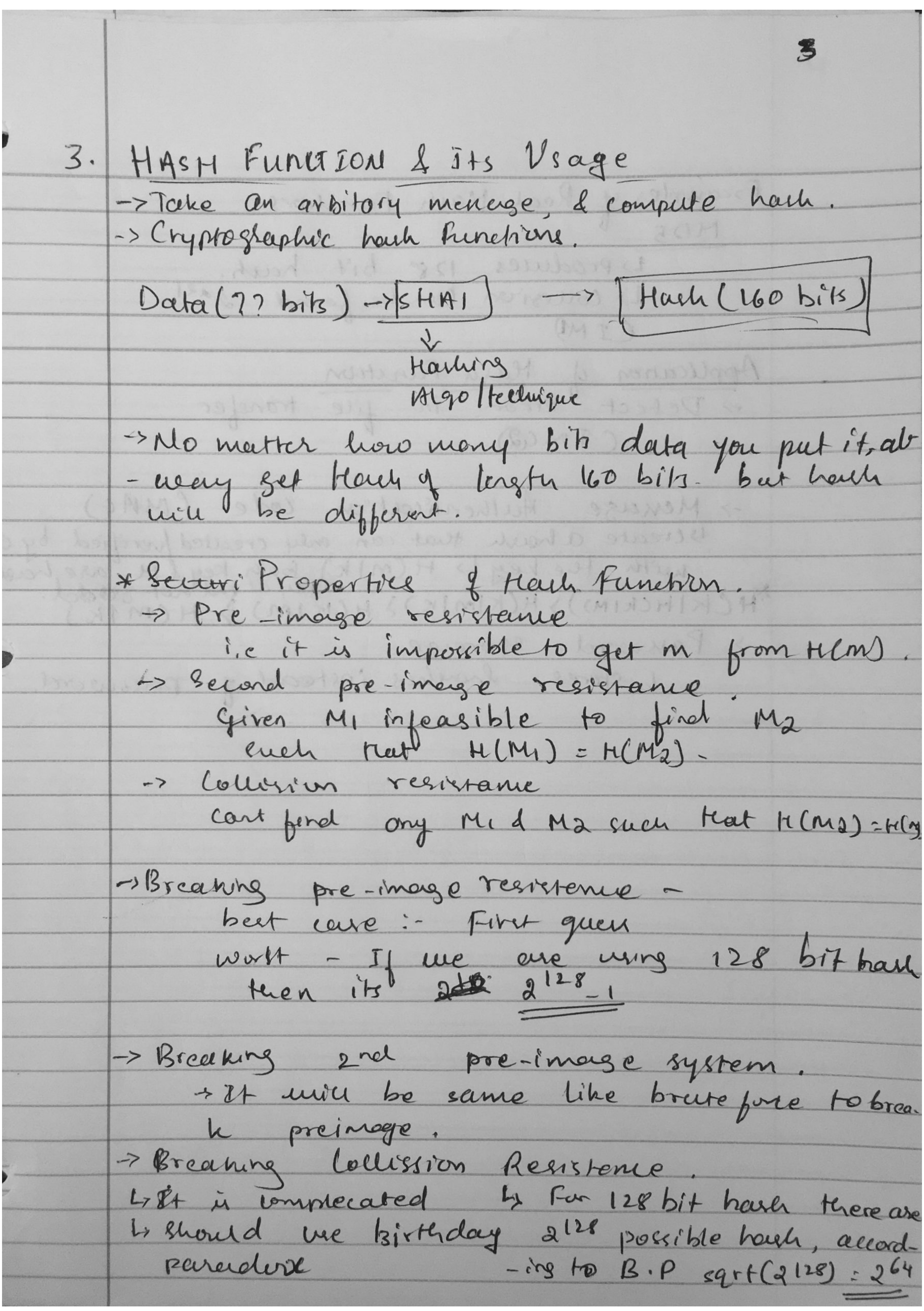
Topic: Hash Function and Its Usage

Course:

Date:

Professor:

Key Points



3

3. HASH FUNCTION & its Usage

-> Take an arbitory message, & compute hash.

-> Cryptographic hash functions.

Data (?? bits) -> SHA1 ⟶ Hash (160 bits)

↓

Hashing Algo/technique

-> No matter how many bits data you put it, al-way get Hash of length 160 bits. but hash will be different.

* Securi Properties of Hash Function.

-> Pre-image resistance

i.e it is impossible to get m from H(m).

-> Second pre-image resistance.

Given M_1 infeasible to find M_2 such that $H(M_1) = H(M_2)$.

-> Collision resistance

Cant find any M_1 & M_2 such that $H(M_1) = H(M_2)$

-> Breaking pre-image resistence -

best case :- First guess

worst - If we are using 128 bit hash then its $2^{128}-1$

-> Breaking 2nd pre-image system.

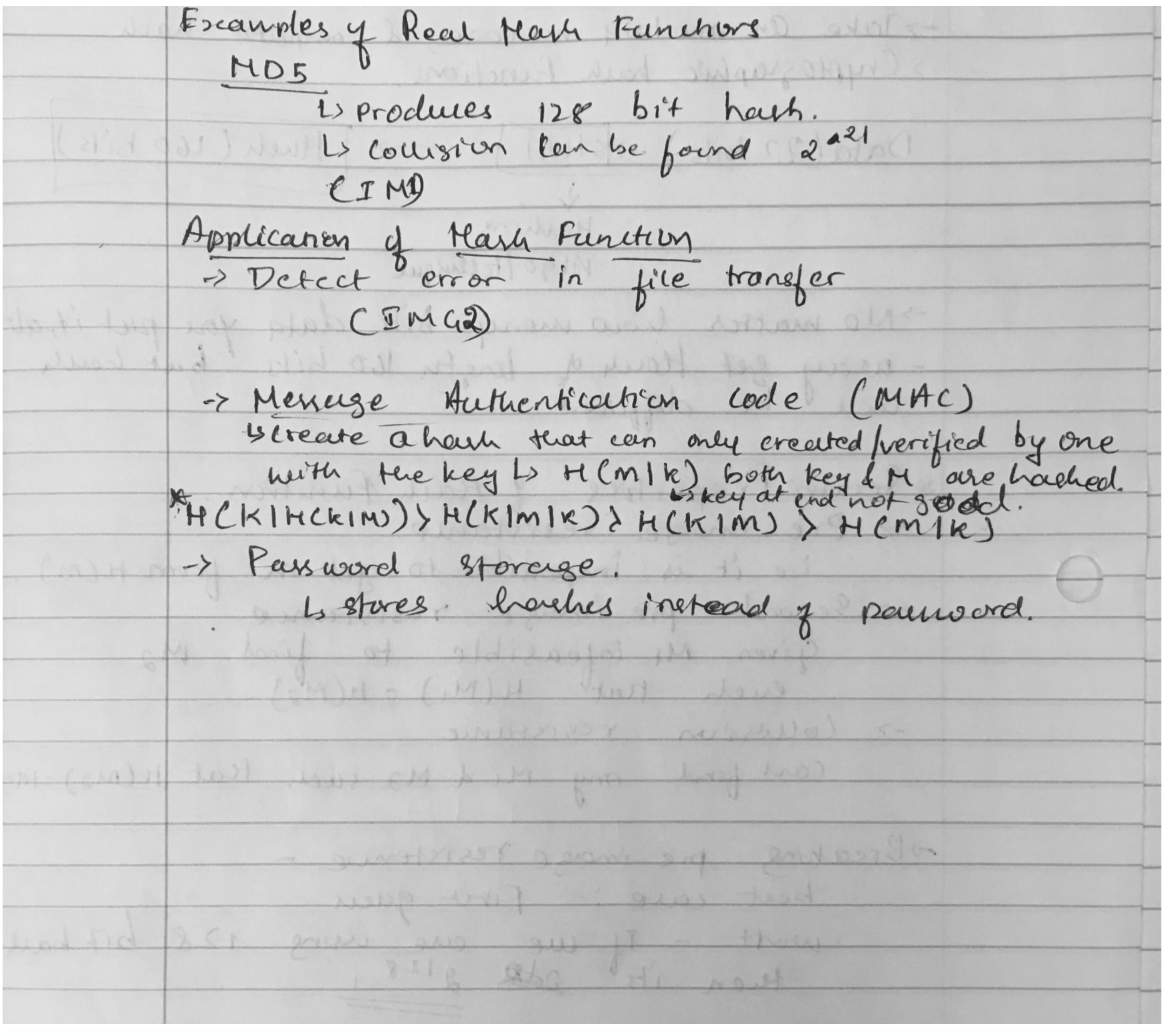
-> It will be same like brute force to break preimage.

-> Breaking Collission Resistence.

↳ It is complecated

↳ should use birthday paradox

↳ For 128 bit hash there are 2^{128} possible hash, accord-ing to B.P sqrt(2^{128}) = 2^{64}



Examples of Real Hash Functions

MD5

↳ Produces 128 bit hash.

↳ collision can be found 2^{21}

(IMG1)

Application of Hash Function

-> Detect error in file transfer

(IMG2)

-> Message Authentication Code (MAC)

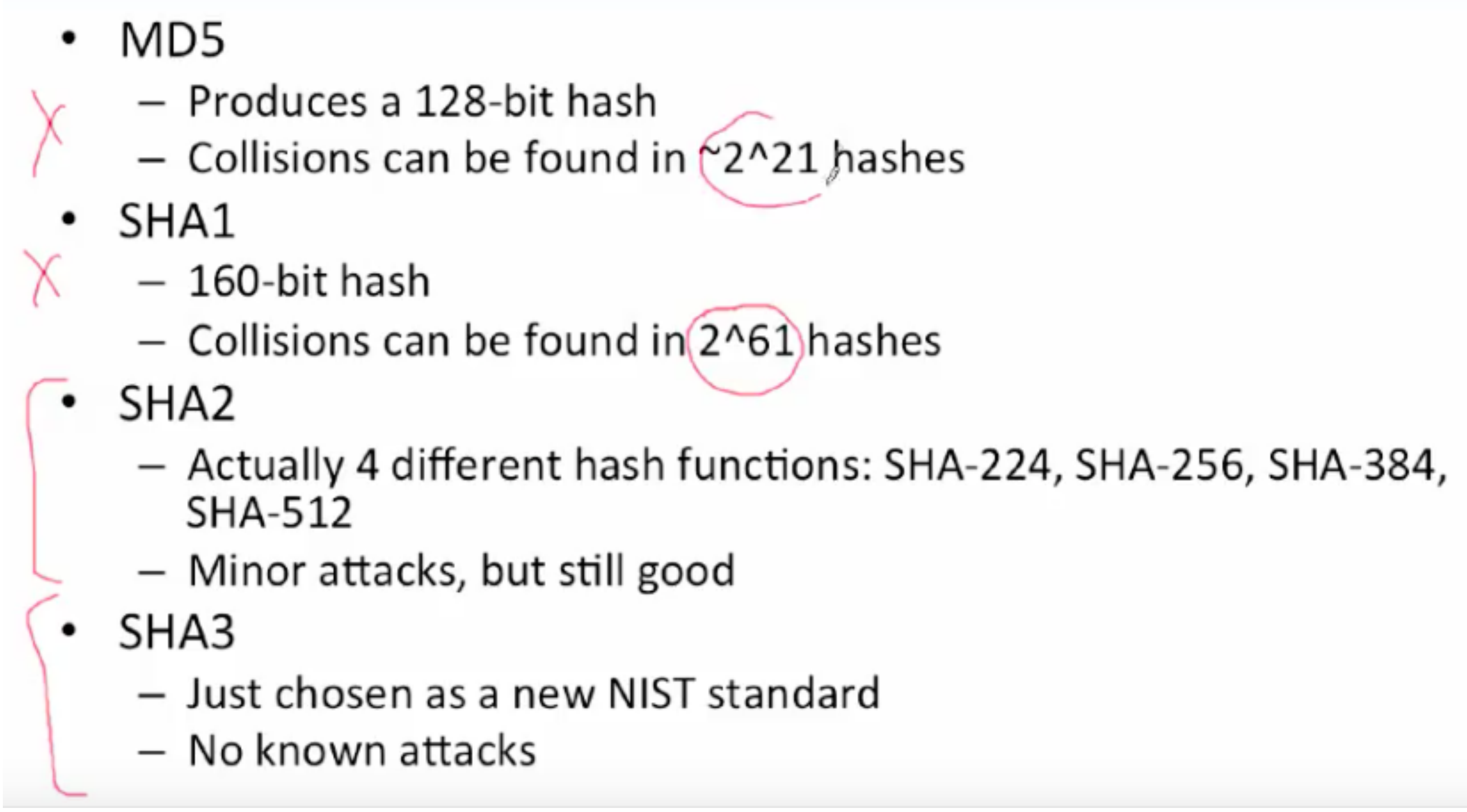
↳ Create a hash that can only created/verified by one with the key ↳ H(m|k) both key & M are hashed.

↳ key at end not good.

* H(K|H(K|M)) > H(K|M|K) > H(K|M) > H(M|K)

-> Password storage.

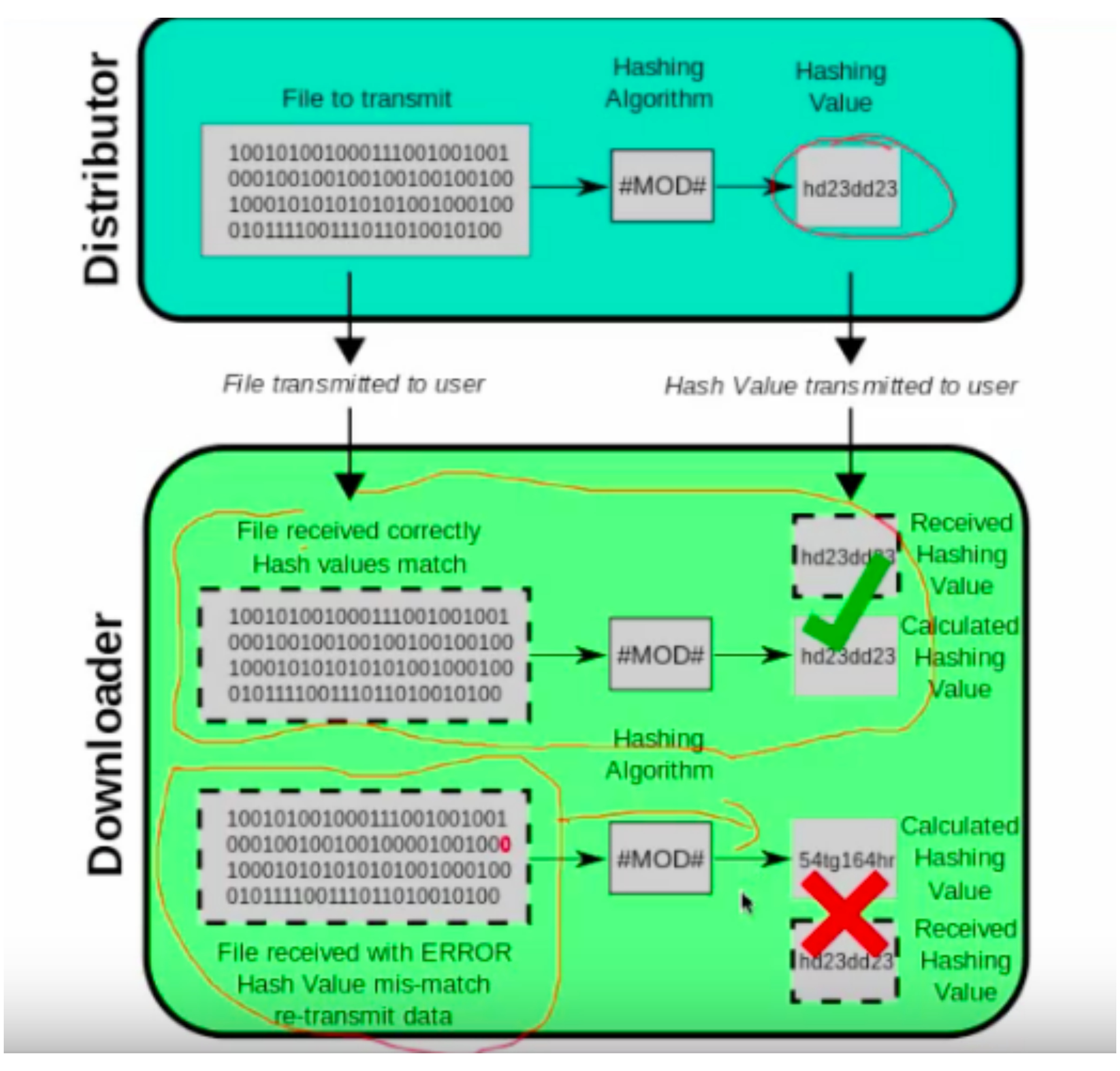
↳ stores hashes instead of password.



- MD5
  - Produces a 128-bit hash
  - Collisions can be found in ~2^21 hashes
- SHA1
  - 160-bit hash
  - Collisions can be found in 2^61 hashes
- SHA2
  - Actually 4 different hash functions: SHA-224, SHA-256, SHA-384, SHA-512
  - Minor attacks, but still good
- SHA3
  - Just chosen as a new NIST standard
  - No known attacks

Application of Hash Functions -

1. Detect error in File Transfer.



Professor's Comment.

I. Properties of Hash Function

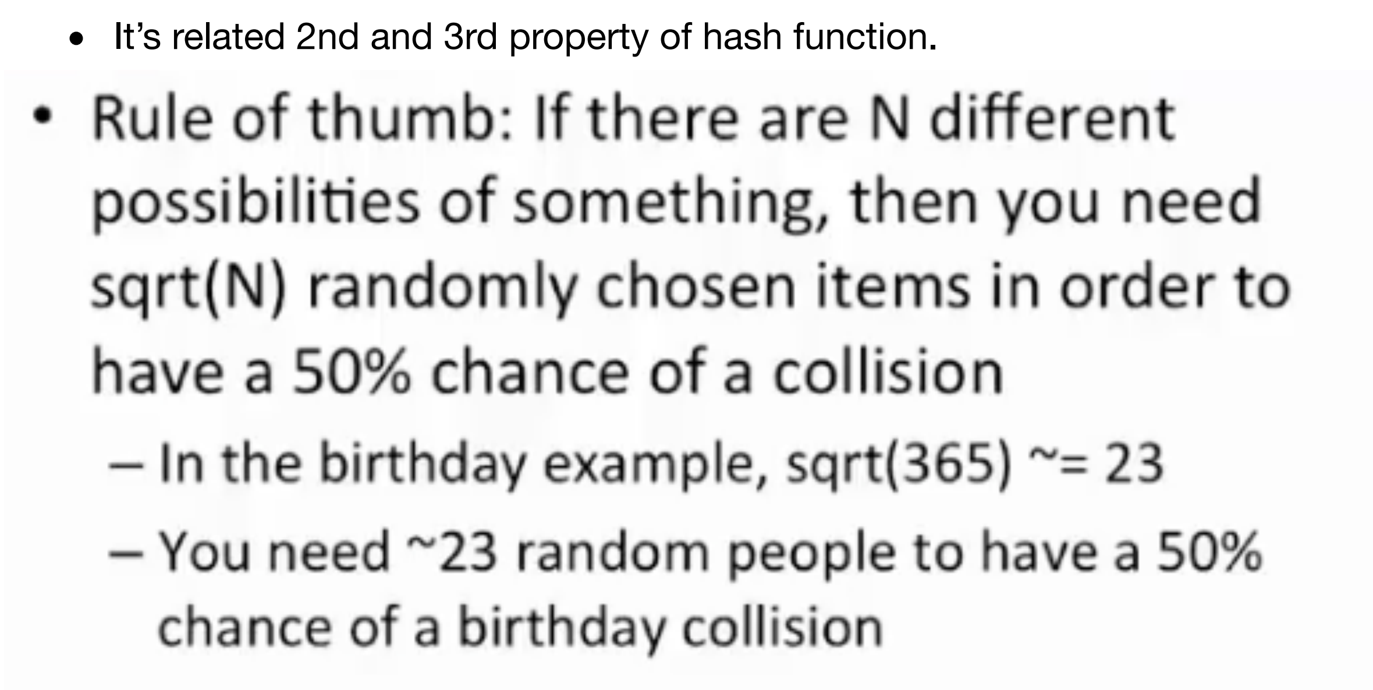
- 1st property is very important and it is one way that means for any given hash it is impossible to find message.
- 3rd property is more stronger than 2nd property.

II. Breaking hashing function

- It is not always true that if we try 2^128 possibilities its not sure that we will get the matching.

III. Birthday Paradox

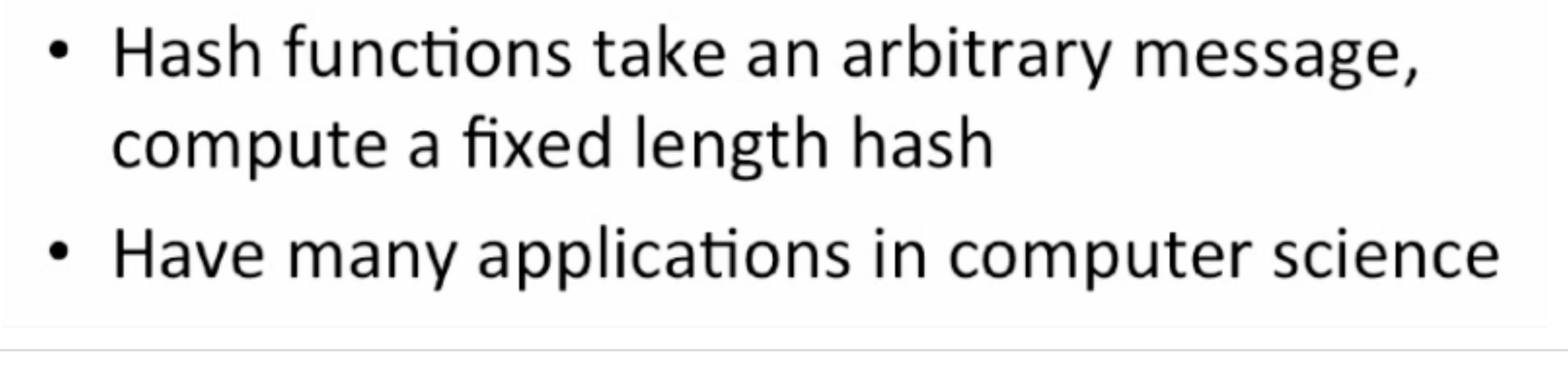
- It's related 2nd and 3rd property of hash function.



- Rule of thumb: If there are N different possibilities of something, then you need sqrt(N) randomly chosen items in order to have a 50% chance of a collision
  - In the birthday example, sqrt(365) ~= 23
  - You need ~23 random people to have a 50% chance of a birthday collision

- Message Authentication Code (MAC) is an important property which allow two parties to communicate securely.

Summary of Notes



- Hash functions take an arbitrary message, compute a fixed length hash
- Have many applications in computer science