CS557: Cryptography

Cryptographic Hash Function

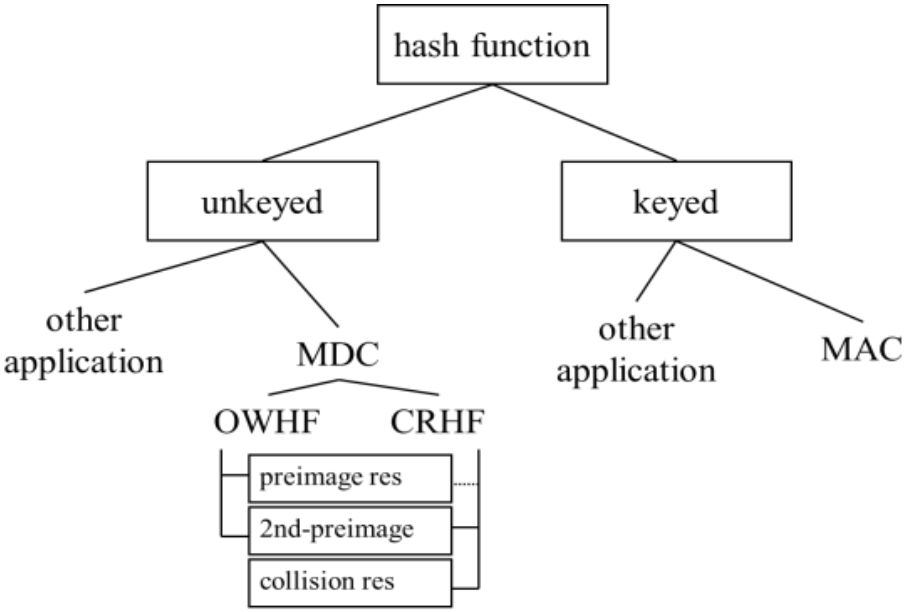
S. Tripathy
IIT Patna

Previous Class

- Cryptography
  - Pseudo Random Number Generator
- Cryptographically Secure PRNGs
  - Blum-Micali Generator
  - Blum-Blum-Shub Generator
- Standardized PRNGs
  - ANSI X9.17 Generator
- Basic Test procedures

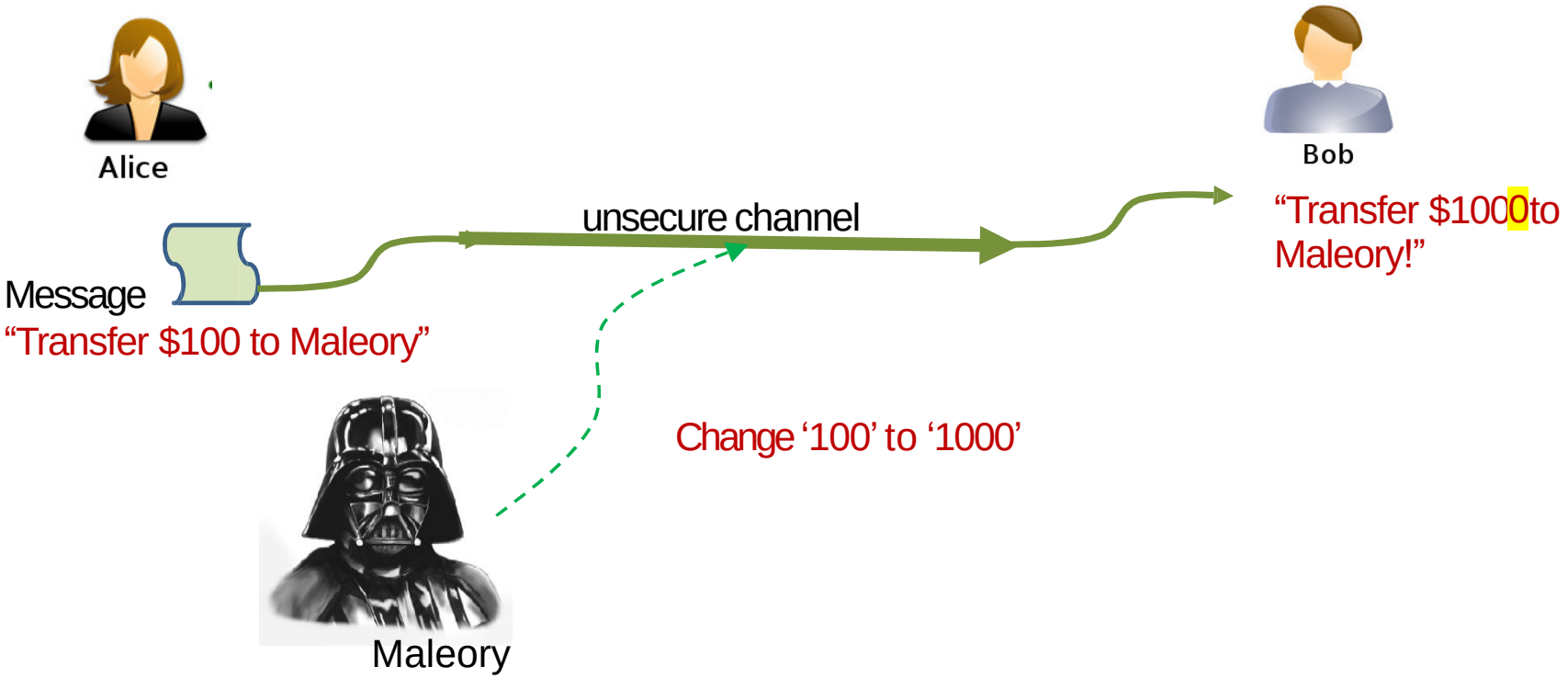
Present Class

- Cryptography
  - Cryptographic Hash Function
    - MD5
    - SHA1



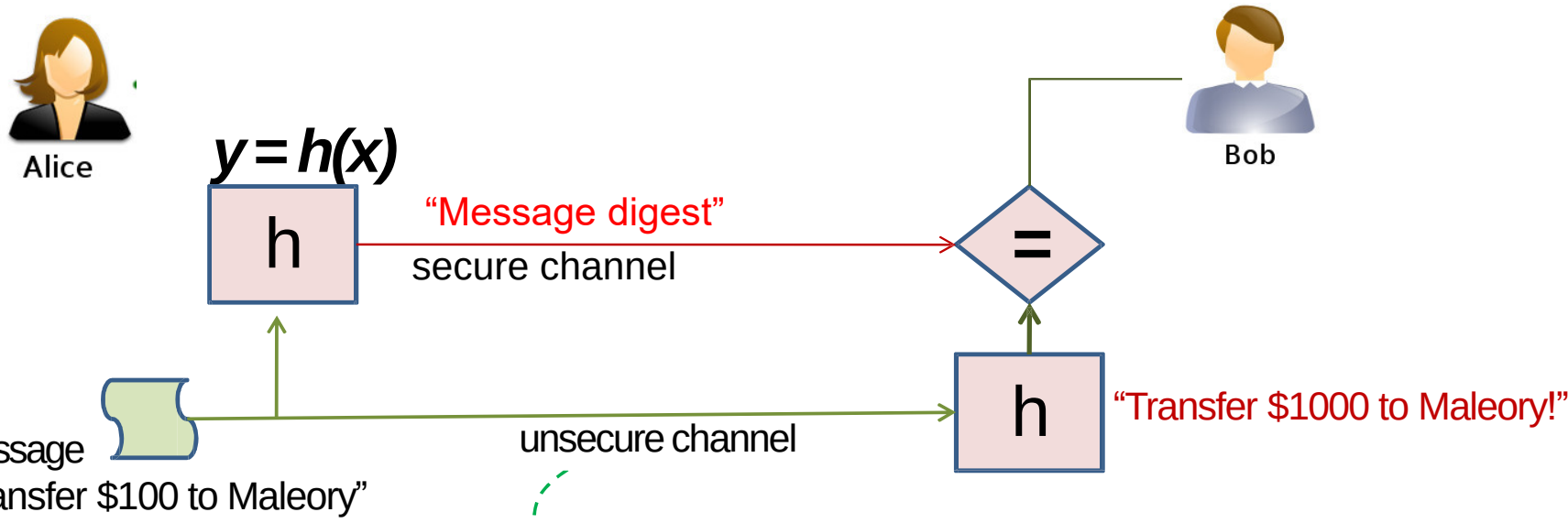
Issues with Integrity

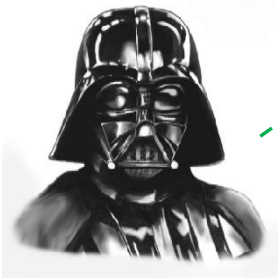
Note…. We are not concerned with confidentiality Now



How can Bob ensure that Alice's message has not been modified ?

Hash (Manipulation Detection code





To suceed

Maleory needs to modify x to x', such that

$h(x) = h(x')$

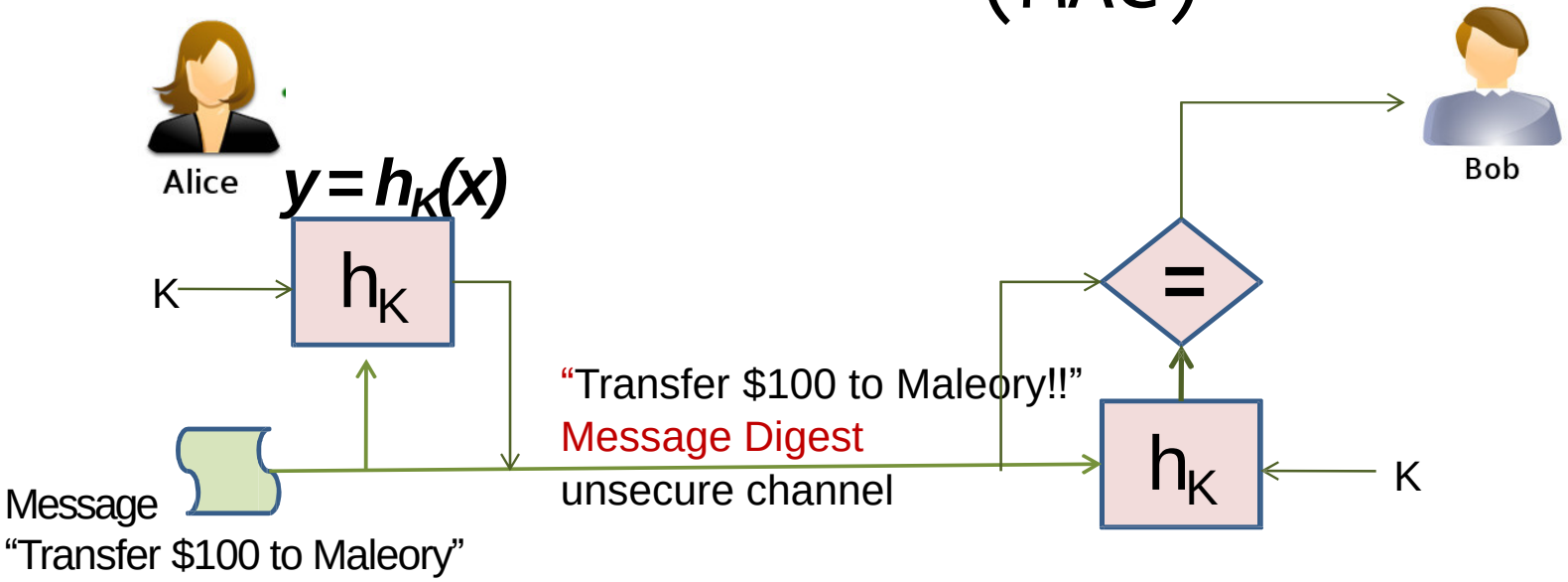
Goal of Hash functions is to resist such collisions

Attacks against MDC

OWHF: given y find x s.t. h(x)=y; or given (x,h(x)) find $x' \neq x$ s.t. h(x')=h(x)

CRHF: find any two inputs $x' \neq x$ s.t. h(x')=h(x) (birthday attack)

Message Authentication Codes (MAC)



MACs can allow the message and the digest to be sent over an insecure channel

However, it requires Alice and Bob to share a common key

Attacks against MAC

without <u>knowing k</u> compute $(x, h_k(x))$ given $(x_i, h_k(x_i))$ with $x_i \neq x$

Applications of Hash functions in Security

- Digital signatures
- Random number generation
- Key updates and derivations
- One way functions
- MAC
- Detect malware in code
- User authentication (storing passwords)

- Thanks