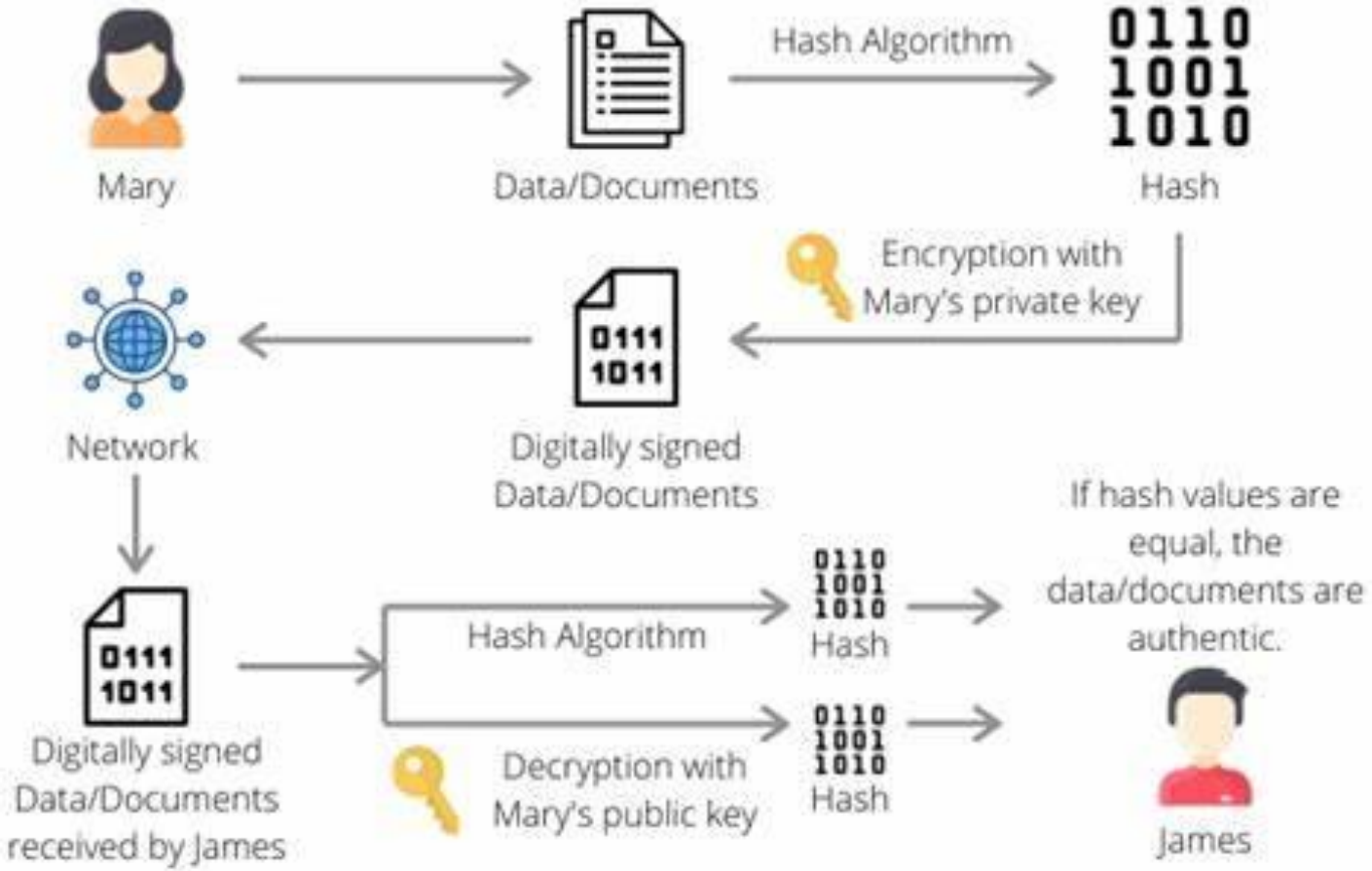
Information Assurance and Security – ACIT 4630

Hesam Alizadeh

Week 6 – Winter 2024

Digital Signature Verification

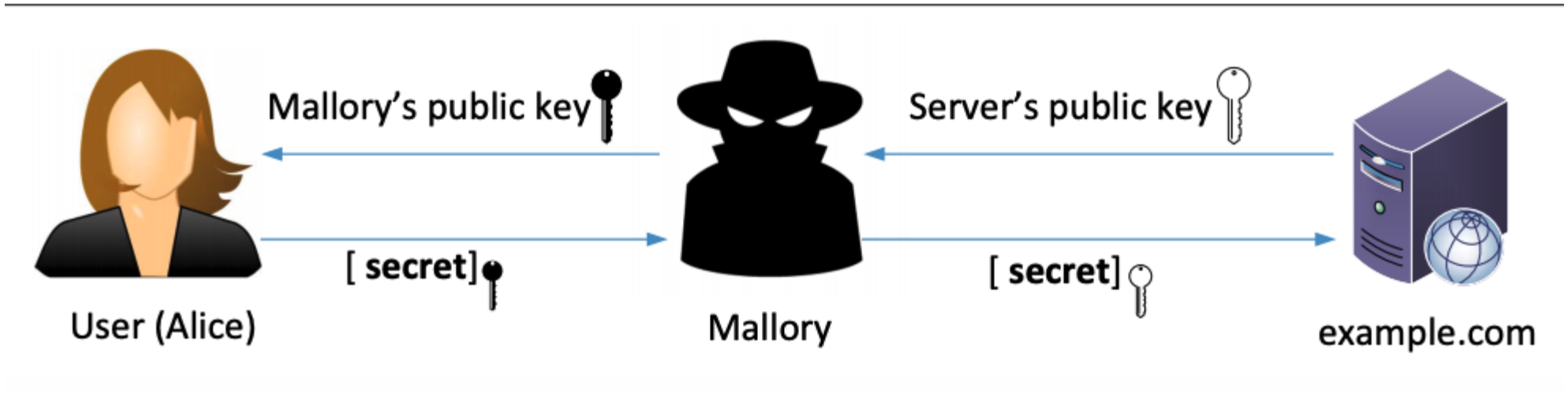
- Digital signatures provide authenticity, integrity, and non-repudiation
- Signer's private key used for **creating** the signature
- Signer's public key used for **verifying** the signature



Source

MITM Attack – Public Key Encryption

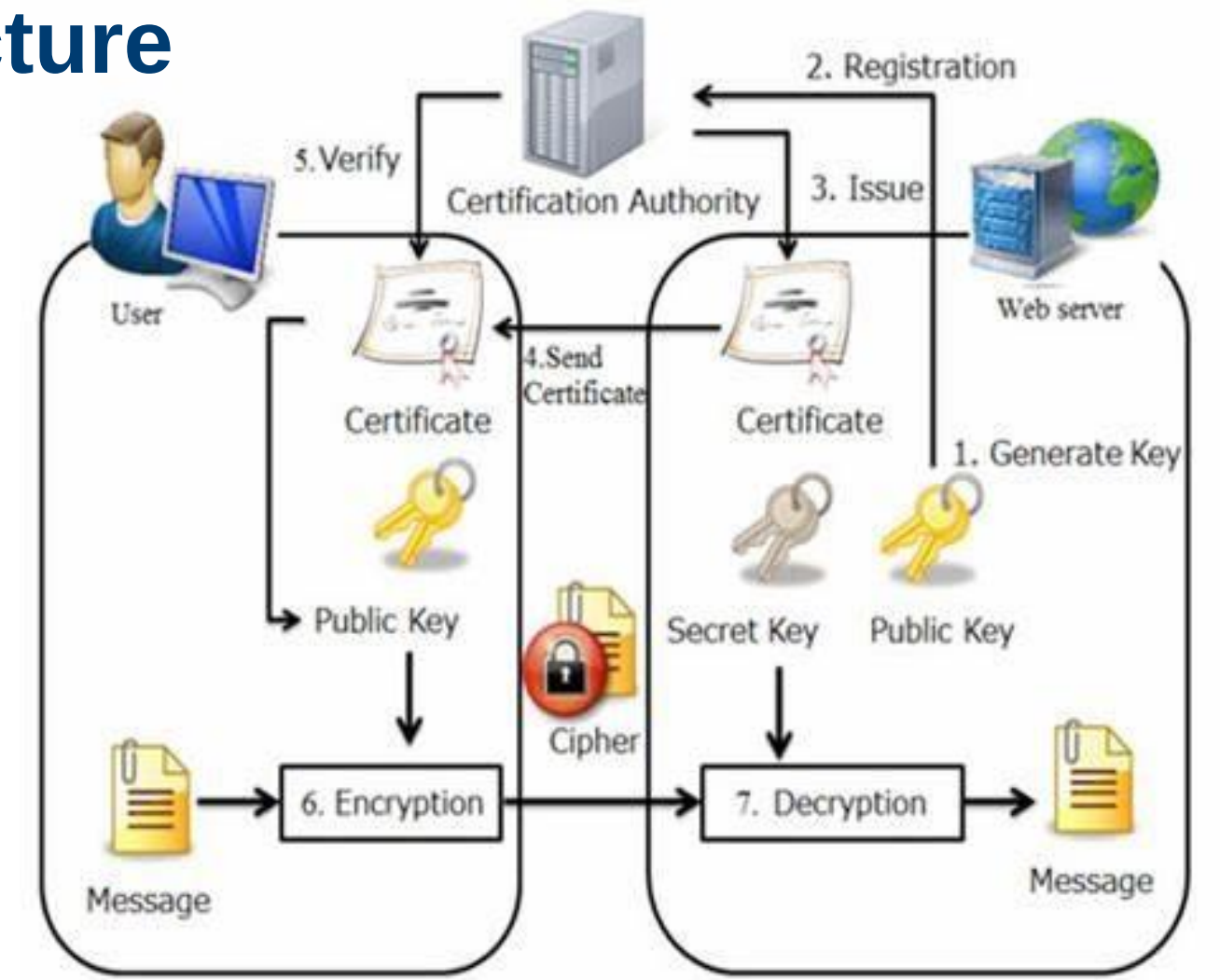
- In asymmetric cryptography the encrypted message can only be decrypted by the recipient's private key
- What if the attacker manipulates the public key during key exchange?



Source

Public Key Infrastructure

- Trusted Certificate Authorities (CA)
  - Verifies identity of users and their public key
  - Issues a digitally signed digital (public key) X.509 certificates



Source