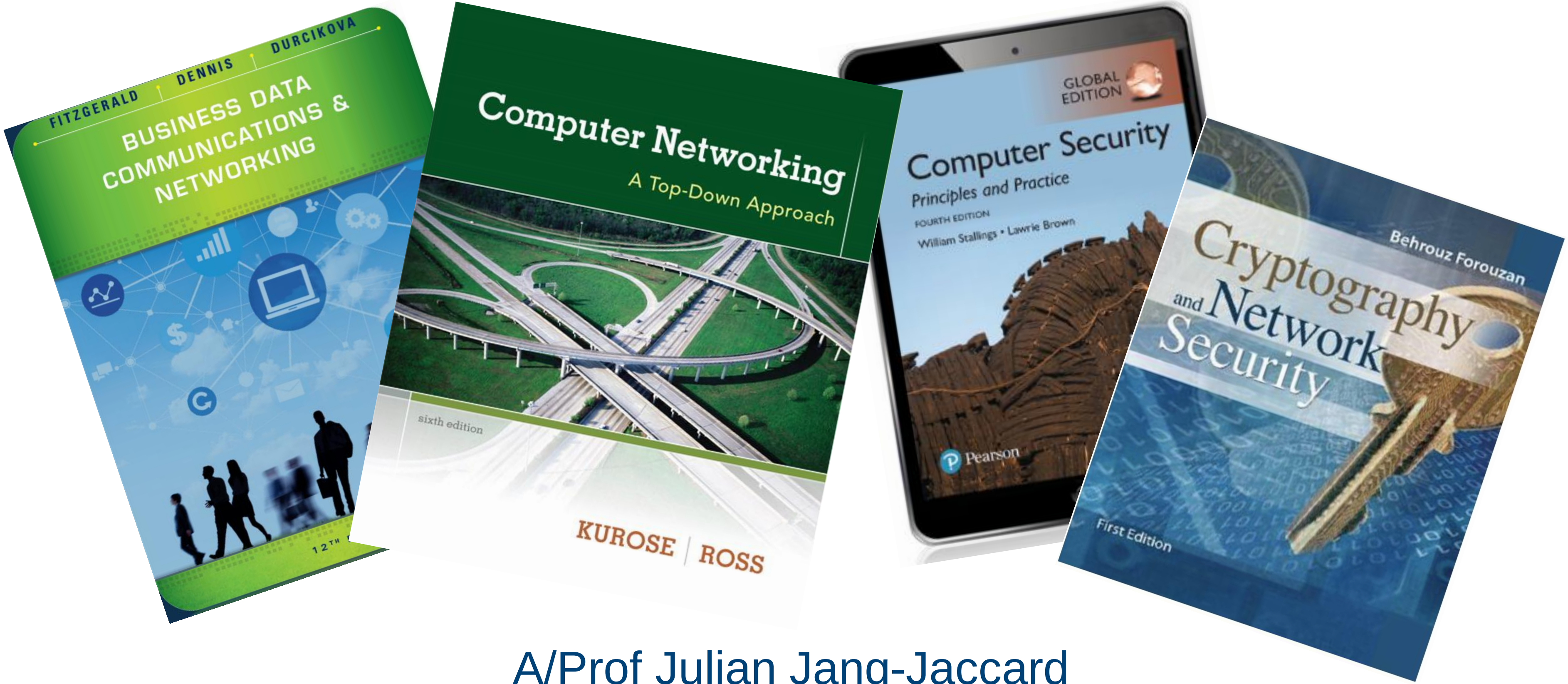
MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Network, Security and Privacy

158.235

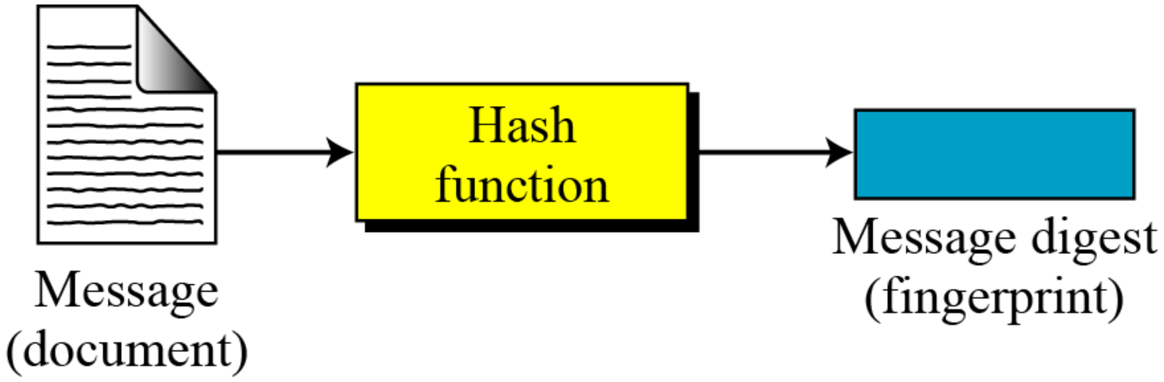


A/Prof Julian Jang-Jaccard

Cryptography continues…

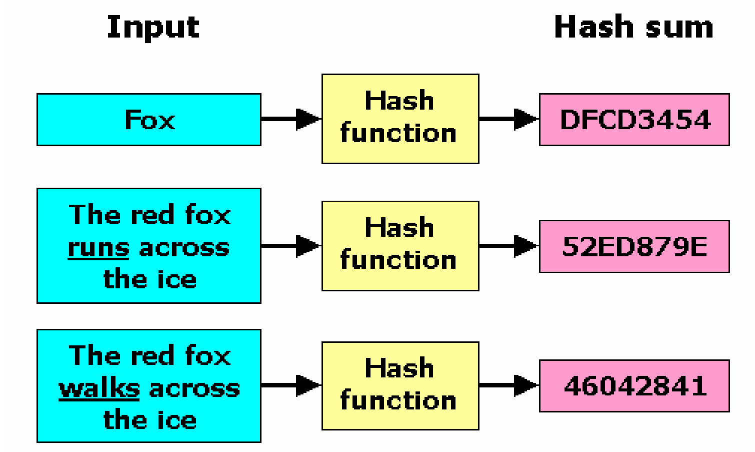
Modern Cryptography

- Two-Way Cryptography
  - Symmetric Cryptography
  - Public key Cryptography
- One-Way Cryptography
  - Hash



Hash Function

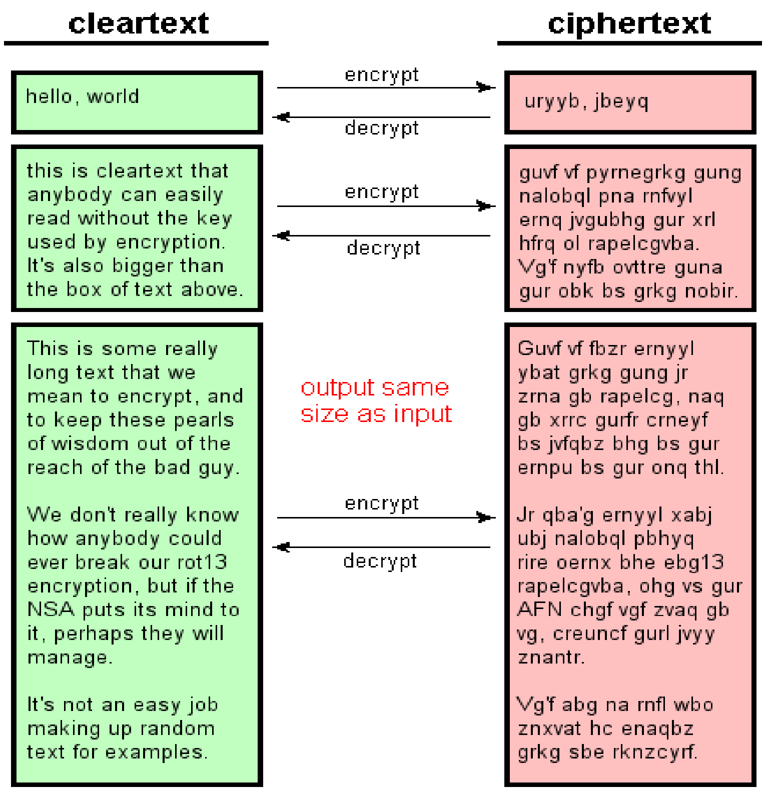
- A hash algorithm creates a unique "digital fingerprint" (= message digest or digest)
- It's a ONE-WAY function
  - Content cannot be used to reveal the original data
  - Takes a variable-length string as input
  - Returns a fixed-length string as output
- Even a small change in the input drastically changes the output
- Primarily for comparison purposes



Hash Functions

- Popular hash function MD5
  - Produce 128-bit ciphertext
  - E.g., b9b985cdc61c8db72289ce54f0937eb2 (32 hex)
  - Thoroughly broken
- Government standard SHA-1, SHA-2
  - SHA-1: 160-bit ciphertext
  - E.g., 4751031b69d5480dfb30023f72640dd45a3c5de (40 hex)
  - Theoretical weaknesses
- “NEW” cryptographic hash function SHA-3
  - Too new to fully evaluate
  - Maybe good enough

Encryption vs. Hash



cleartext

ciphertext

hello, world

encrypt

decrypt

uryyb, jbeyq

this is cleartext that anybody can easily read without the key used by encryption. It's also bigger than the box of text above.

encrypt

decrypt

guvf vf pyrnegrkg gung nalobql pna rnfvyl ernq jvgubhg gur xrl hfrq ol rapelcgvba. Vg'f nyfb ovttre guna gur obk bs grkg nobir.

This is some really long text that we mean to encrypt, and to keep these pearls of wisdom out of the reach of the bad guy.

We don't really know how anybody could ever break our rot13 encryption, but if the NSA puts its mind to it, perhaps they will manage.

It's not an easy job making up random text for examples.

output same size as input

encrypt

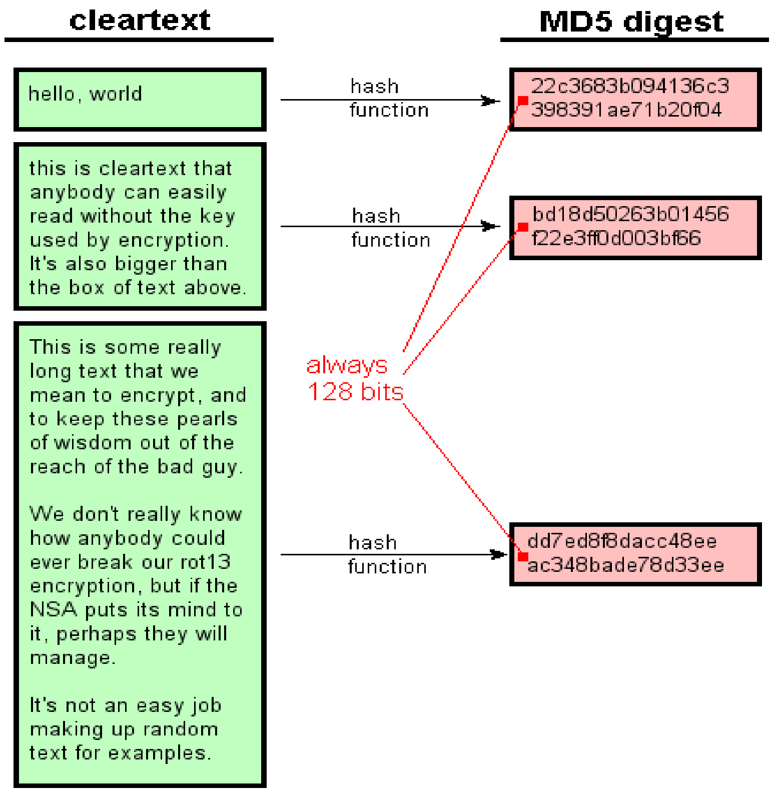
decrypt

Guvf vf fbzr ernyyl ybat grkg gung jr zrna gb rapelcg, naq gb xrrc gurfr crneyf bs jvfqbz bhg bs gur ernpu bs gur onq thl.

Jr qba'g ernyyl xabj ubj nalobql pbhyq rire oernx bhe ebg13 rapelcgvba, ohg vs gur AFN chgf vgf zvaq gb vg, creuncf gurl jvyy znantr.

Vg'f abg na rnfl wbo znxvat hc enaqbz grkg sbe rknzcyrf.

Fig. 1: Encryption - a two-way operation



cleartext

MD5 digest

hello, world

hash function

22c3683b094136c3 398391ae71b20f04

this is cleartext that anybody can easily read without the key used by encryption. It's also bigger than the box of text above.

hash function

bd18d50263b01456 f22e3ff0d003bf66

This is some really long text that we mean to encrypt, and to keep these pearls of wisdom out of the reach of the bad guy.

We don't really know how anybody could ever break our rot13 encryption, but if the NSA puts its mind to it, perhaps they will manage.

It's not an easy job making up random text for examples.

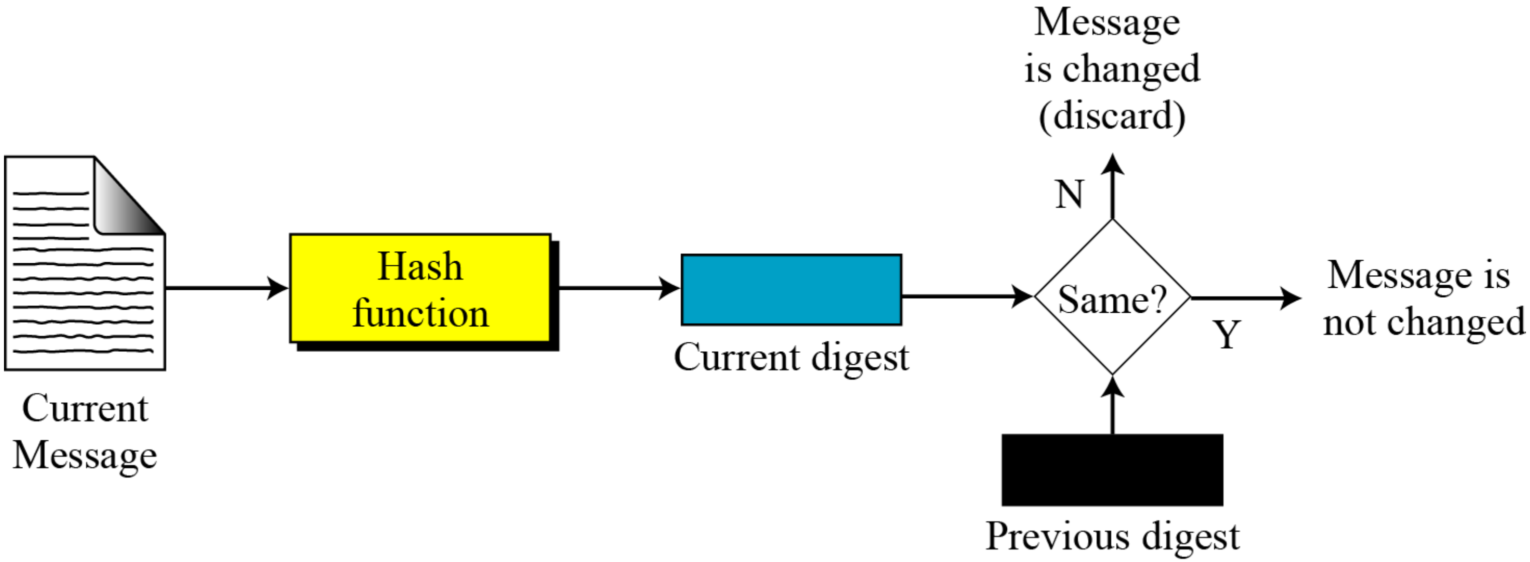
always 128 bits

hash function

dd7ed8f8dacc48ee ac348bade78d33ee

Fig. 2: Hashing - a one-way operation

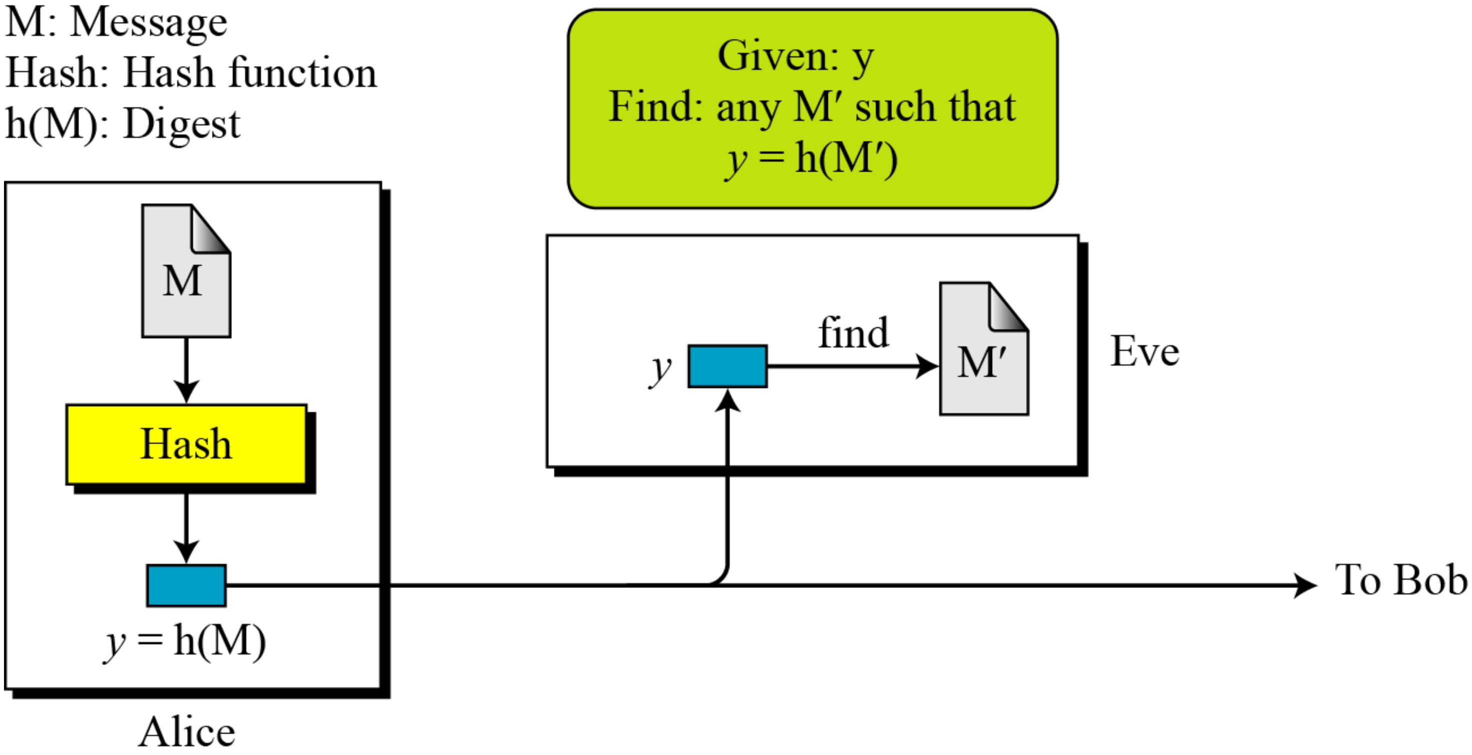
Checking Integrity



Hash Characteristics: Preimage Resistance

Preimage Attack

Given: y = h(M) **Find: M′ such that y = h(M′)**



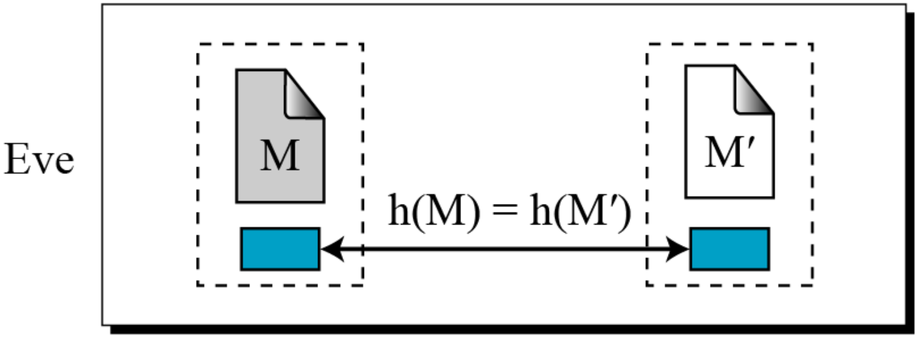
Hash Characteristics: Collision Resistance

Collision Attack

Given: none **Find: $M' \neq M$ such that $h(M) = h(M')$**

M: Message
Hash: Hash function
h(M): Digest

Find: M and M′ such that $M \neq M'$, but $h(M) = h(M')$

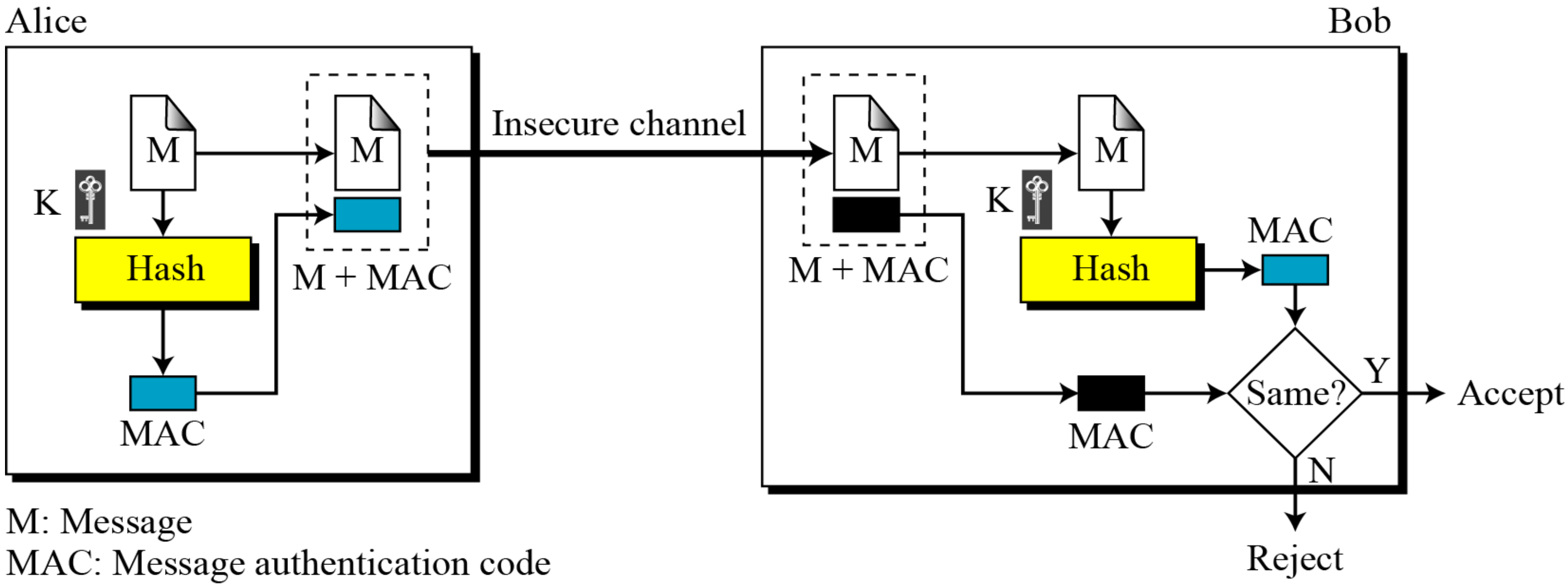


Hash: Summary

- Fixed Size.
  - Always produce the same fixed size output no matter how long the input is.
- Unique.
  - Two different sets of data cannot produce the same digest
  - Known as a collision
- Original.
  - Should not be possible to produce a desired or predefined hash
- Secure.
  - The resulting hash cannot be reversed in order to determine the original words

Message Authentication Code (MAC)

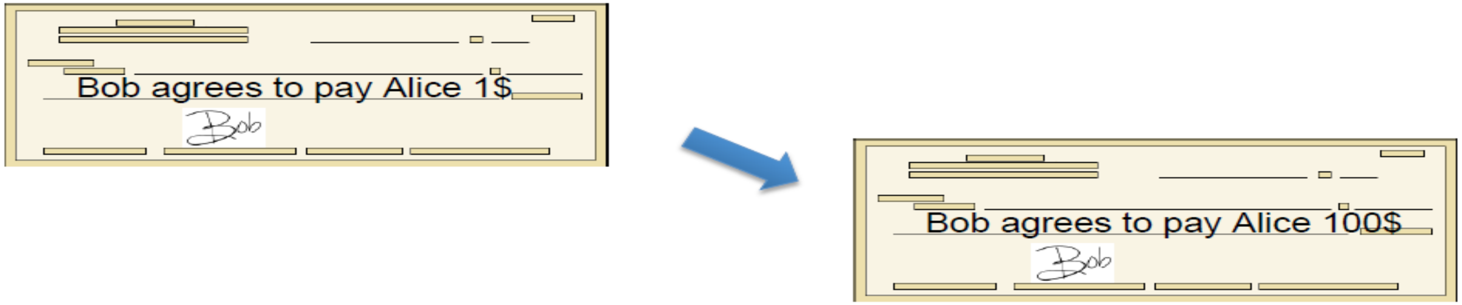
- Is a mechanism used to authenticate the sender of the message



M: Message
MAC: Message authentication code
K: A shared secret key

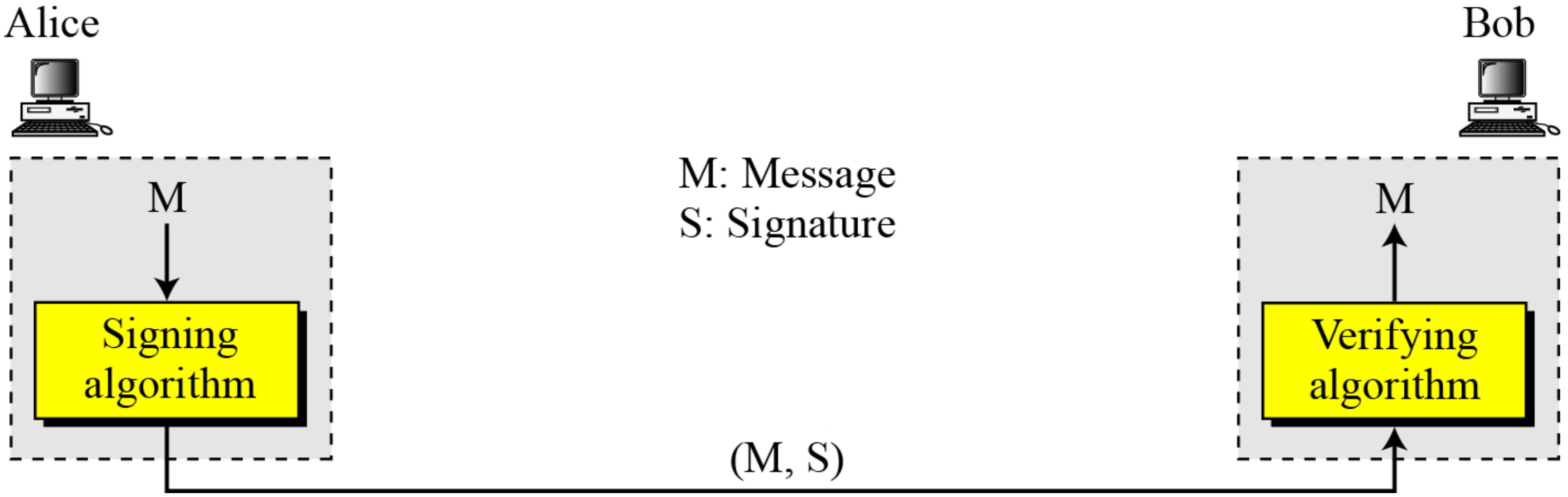
Digital Signatures

- cryptographic technique analogous to hand-written signatures
- Sender (Bob) digitally signs document, establishing he is document owner/creator.
- Verifiable, non-forgeable: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document



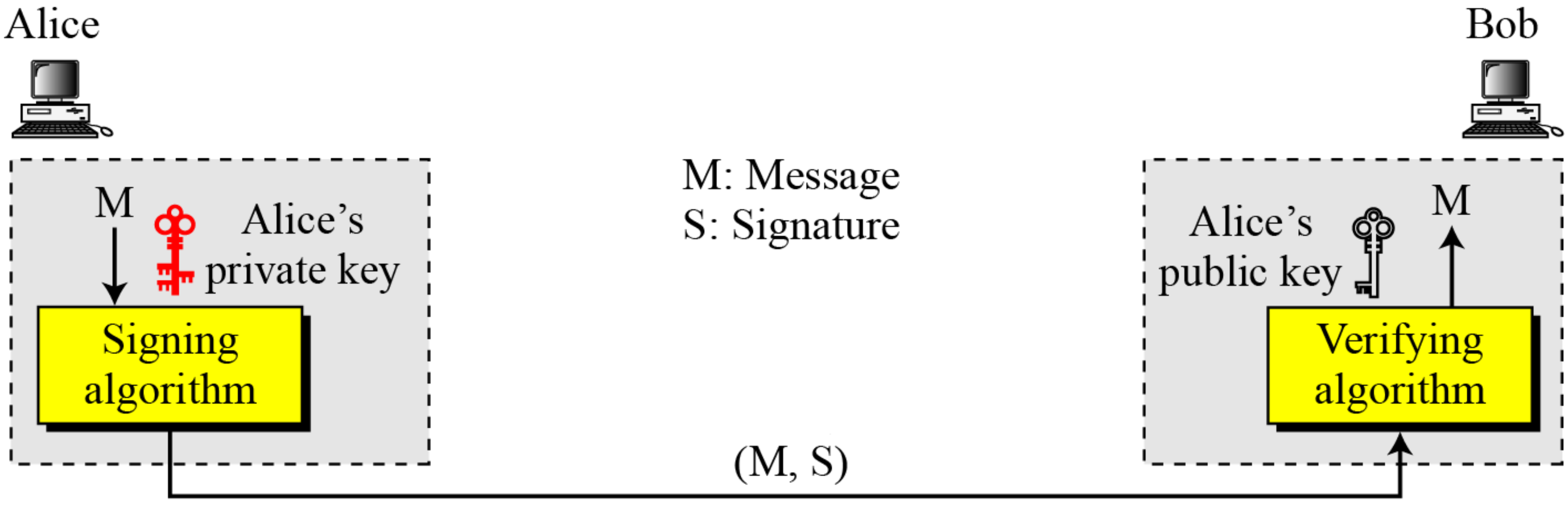
Digital Signatures

- The sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver.
- The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted; otherwise, it is rejected.



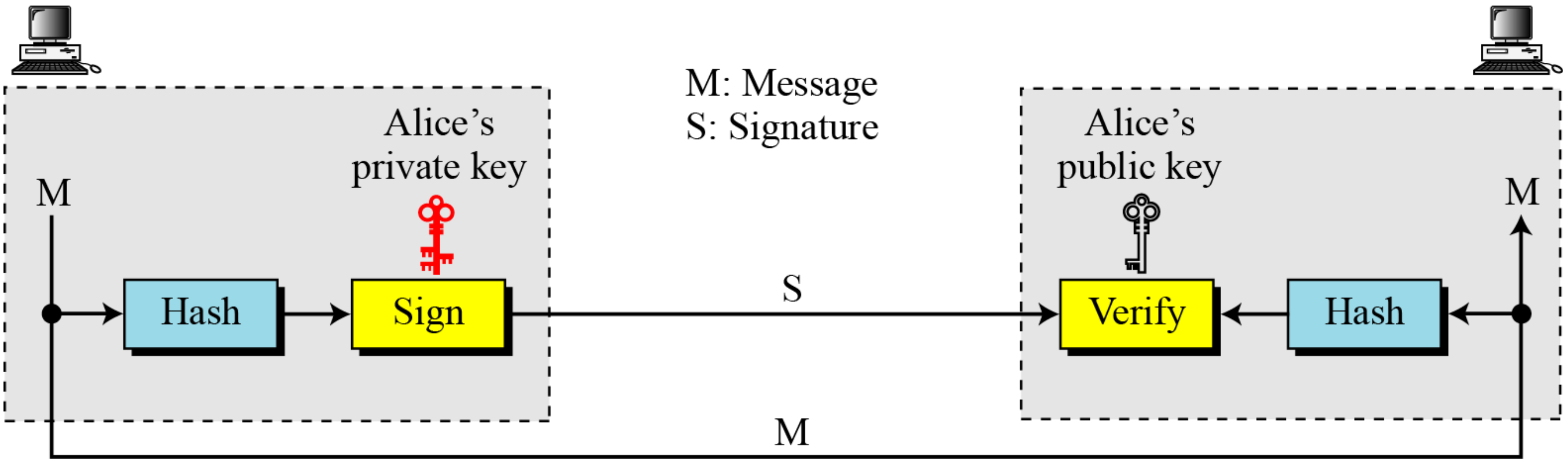
Digital Signatures

- A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.



Signing the Digest

- Sender’s Side: A hash is created for the sender’s message. It is the hash that is signed by the private key of the sender (= digital signature). The original message and the digital signature is sent to the receiver.
- Receiver’s Side: Digital signature is verified by decrypting it with the sender’s public key which reveals the hash. A hash value of the message transmitted to the recipient is created and compared with the hash from the digital signature



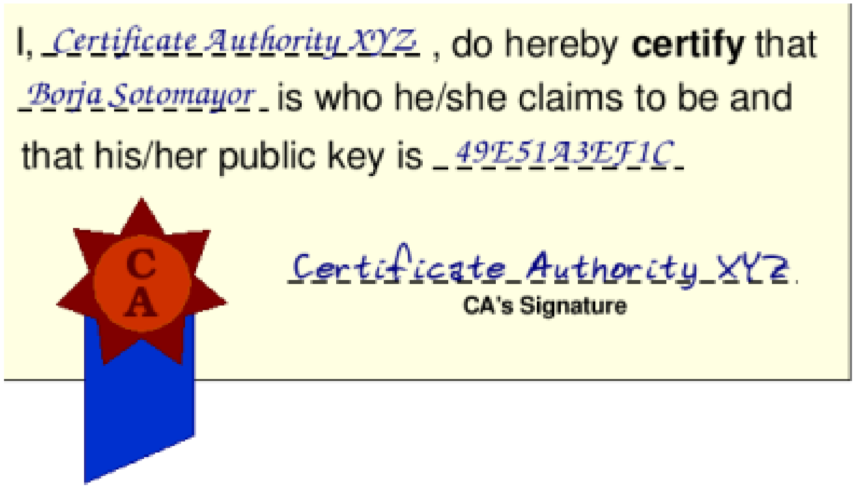
Key Comparisons

Security Goal	Hash	MAC	Digital Signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Key	None	Symmetric keys	Asymmetric keys

- Integrity – guarantee no unauthorised modification/deletion happened
- Authentication – proving who you are (did you send that message?)
- Non-repudiation – cannot deny knowledge of an action done by a user (I never sent that message to Julian)

Digital Certificate

- Problem: How to trust that a public key belong to whom it claims to be?
- Solution: Use trusted third-party entity. They vouch that a public key belongs to a particular individual or organization

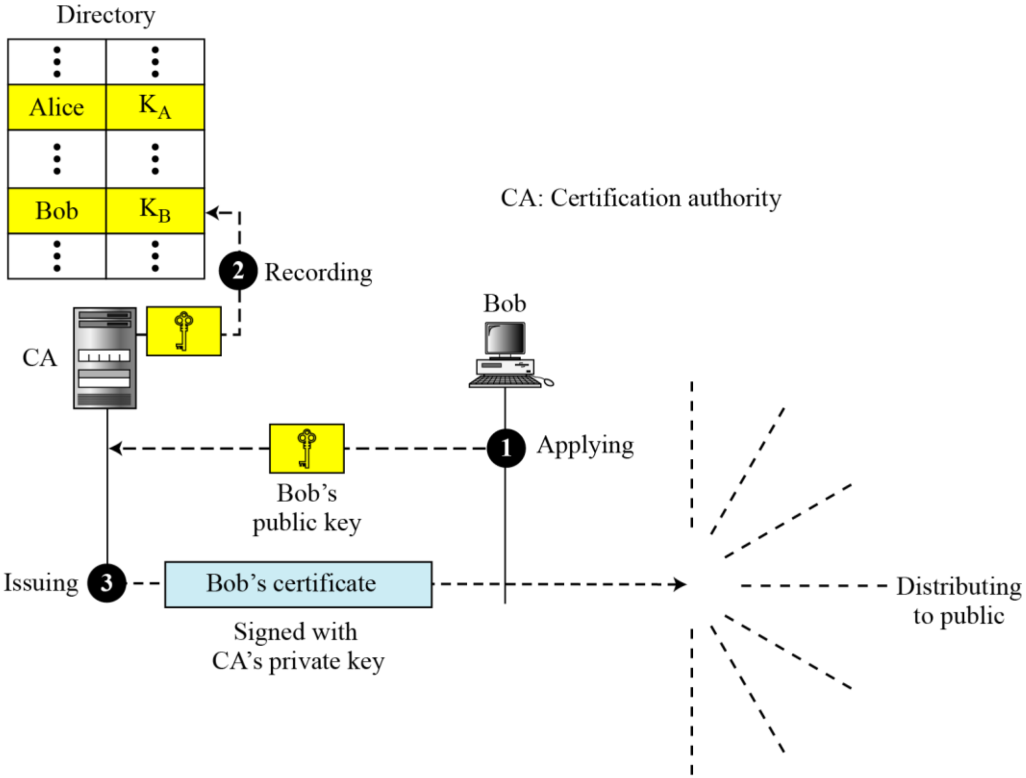


I, Certificate Authority XYZ , do hereby **certify** that Borja Sotomayor is who he/she claims to be and that his/her public key is 49E51A3EF1C

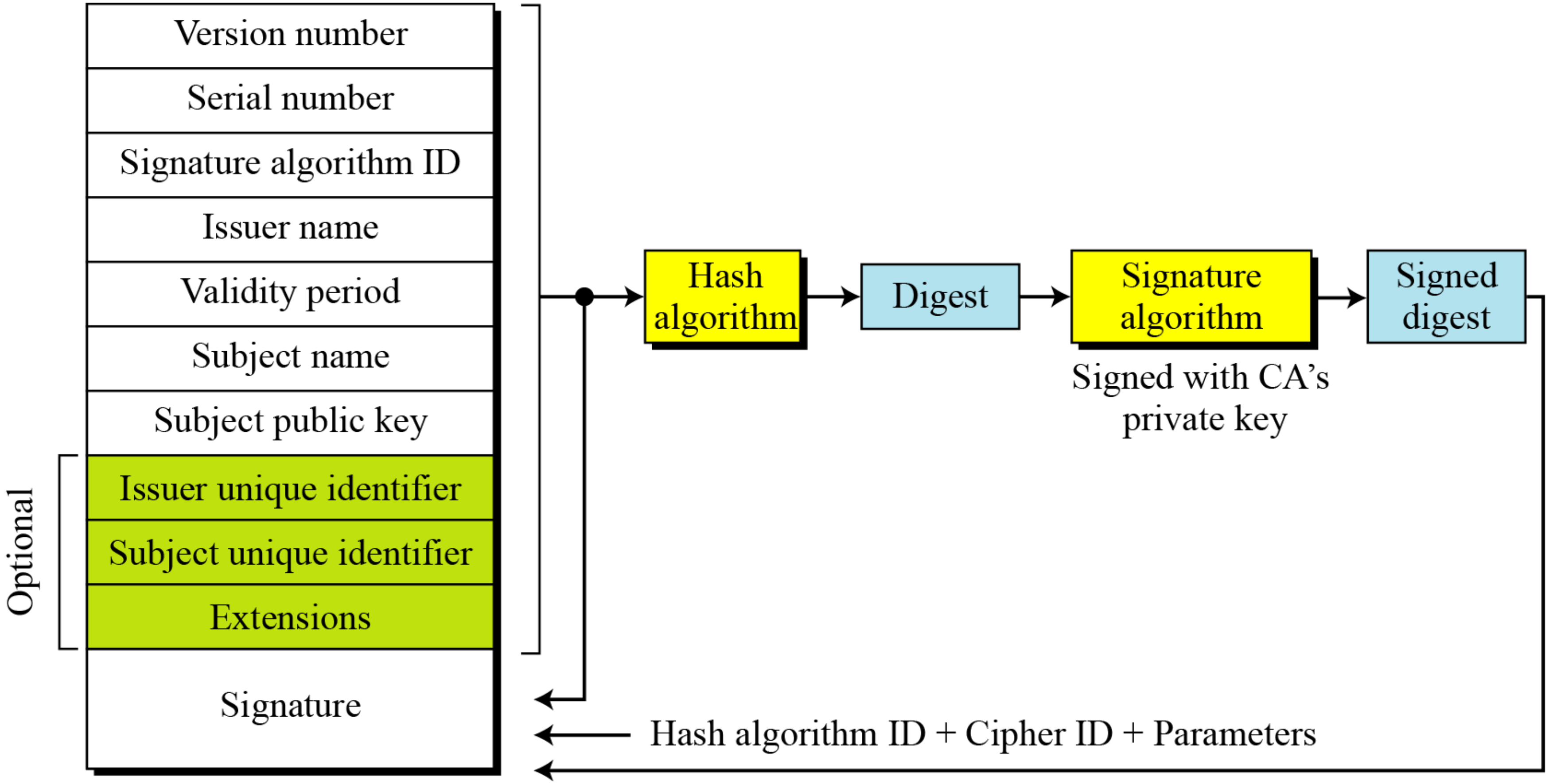
Certificate Authority XYZ
CA's Signature

Certification Authority (CA)

- CA issues the certification – signed with CA's private key
- Each certificate has a period of validity. If there is no problem with the certificate, the CA issues a new certificate before the old one expires.



X.509 Certificate



Public Key Infrastructure (PKI)

- Set of hardware, software, organizations, and policies to make Public Key Cryptography work on Internet
  - How to verify that the person sending the message
- User registers with a CA (e.g. VeriSign) and requests for an X.509 certificate
  - a Certificate Signing Request (CSR) is sent to CA
  - Must provide some proof of Identity
  - Levels of certification: simple email confirmation or background checks
- CA issues the digital certificate (signed by CA)
- User attaches the certificate to transactions (email, web, etc)
- Receiver authenticates transaction with CA's public key
  - Contact CA to ensure the certificate is not revoked or expired

MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

END