DIGITAL SIGNATURE

David Yang

BIT 801

April 8, 2008

What is a Digital Signature?

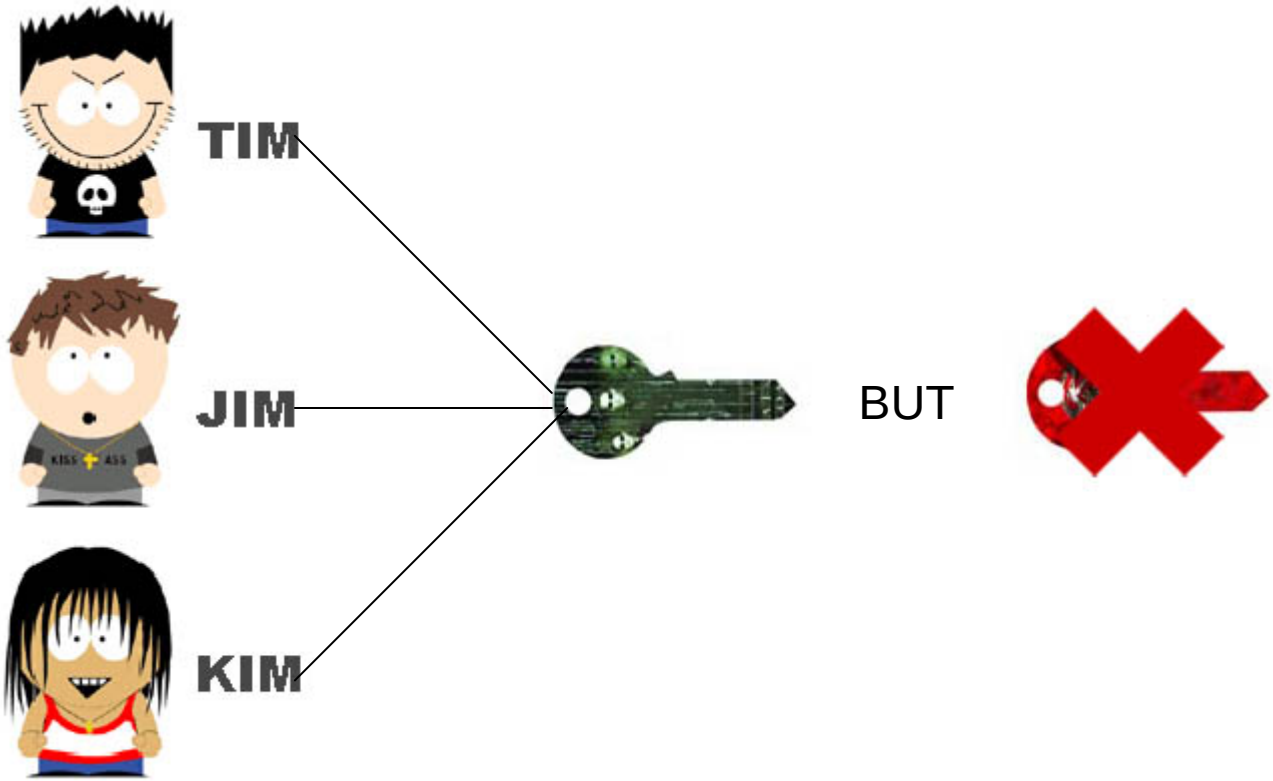
DAVE

Private

Public

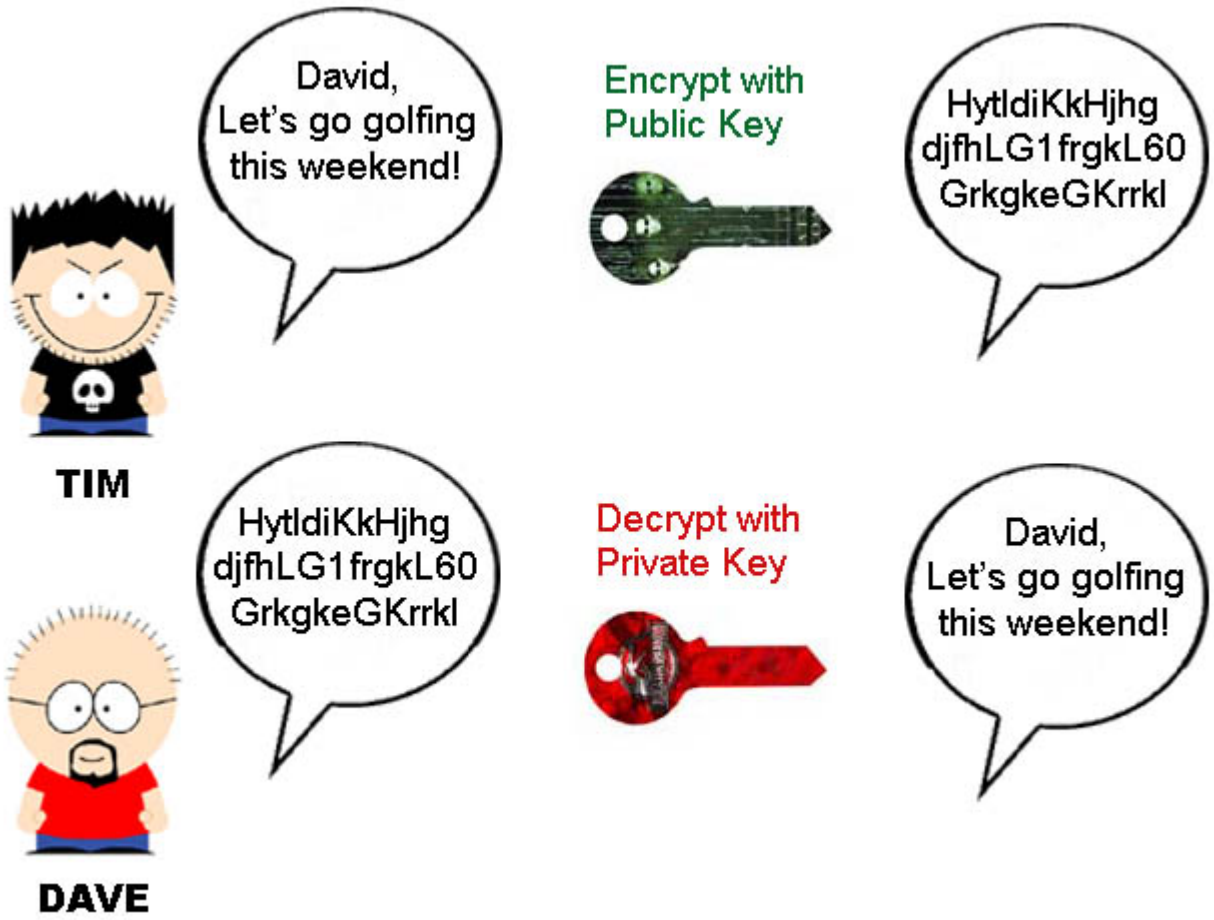
Dave was given 2 keys. A public key and a private key

What is a Digital Signature?



Dave's public key (green) is available to all his colleagues, Tim, Jim, and Kim, but he keeps his private key (red) to himself.

What is a Digital Signature?



What is a Digital Signature?

A Digital Signature is

- a “stamp” put on the data.
- unique to Dave.
- hard to counterfeit.
- guarantees modification made cannot be undetected.

The text books define Digital Signature as follows:

“Digital signatures are designed to bind the message originator with the exact contents of the message.” ----- Greenstein

“A digital signature is basically digital code that is appended to an email.”

----- Greene

“Digital signatures are encrypted message that are independently verified as authentic by a central facility.” ----- Whitman & Battord

What is a Digital Signature?

HASH FUNCTION

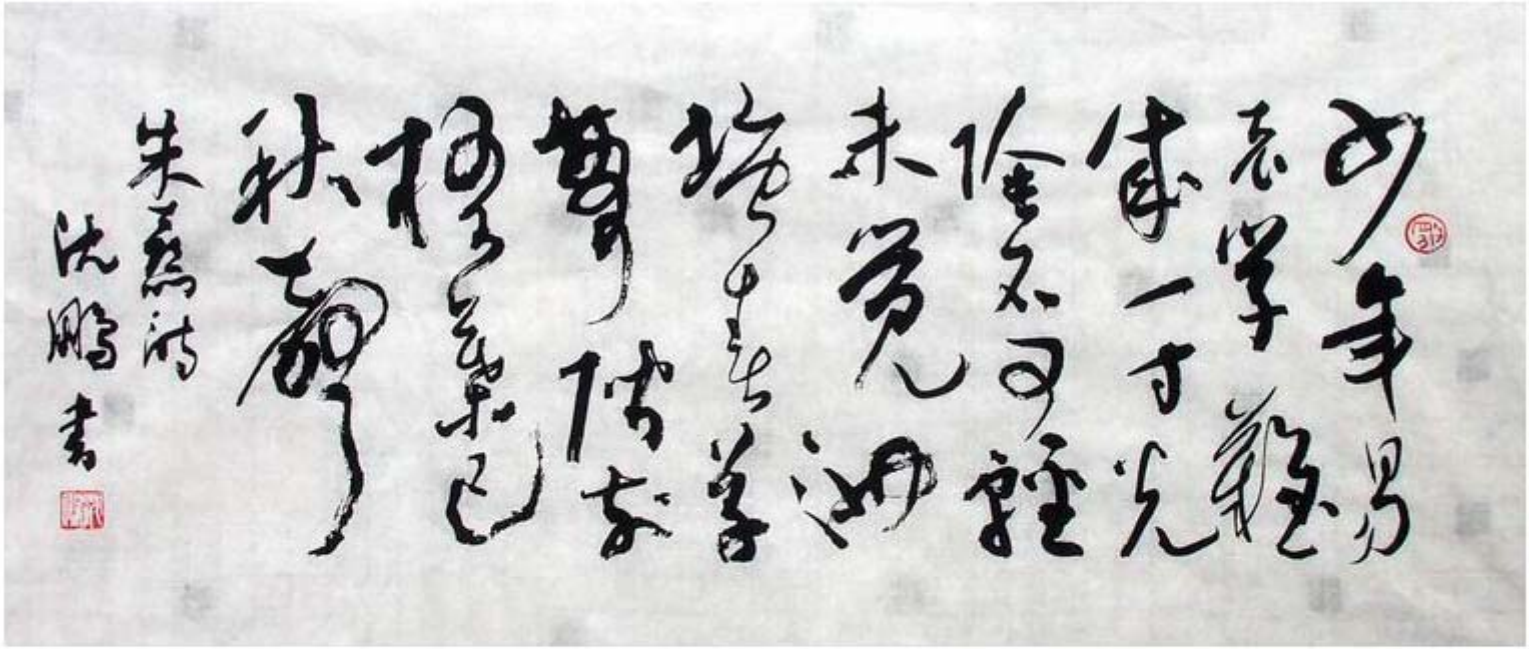
- transforms (encrypts) a plain text into a message digest
- turns a variable-length input to a fixed-length output

  (output size < input size)

MESSAGE DIGEST

- the same plaintext through the same hash function turns out to be the same message digest
- if different, then message has been tampered with during the transport, therefore, the content must not be trusted!

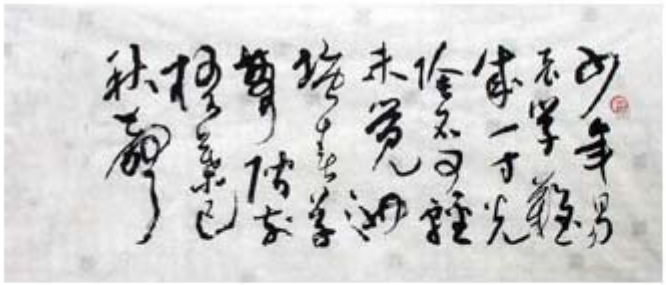
How to Send with Digital Signature?

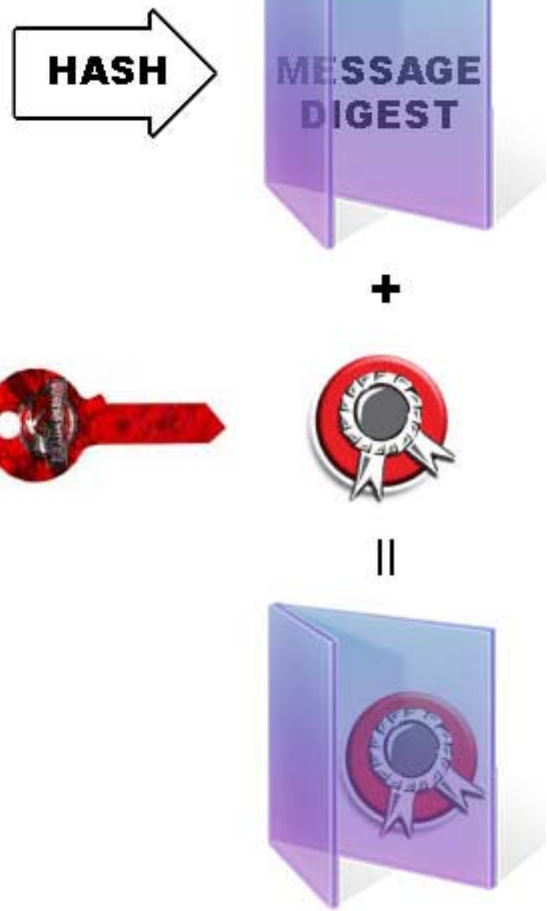


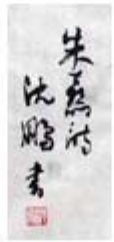
SENDER

RECEIVER

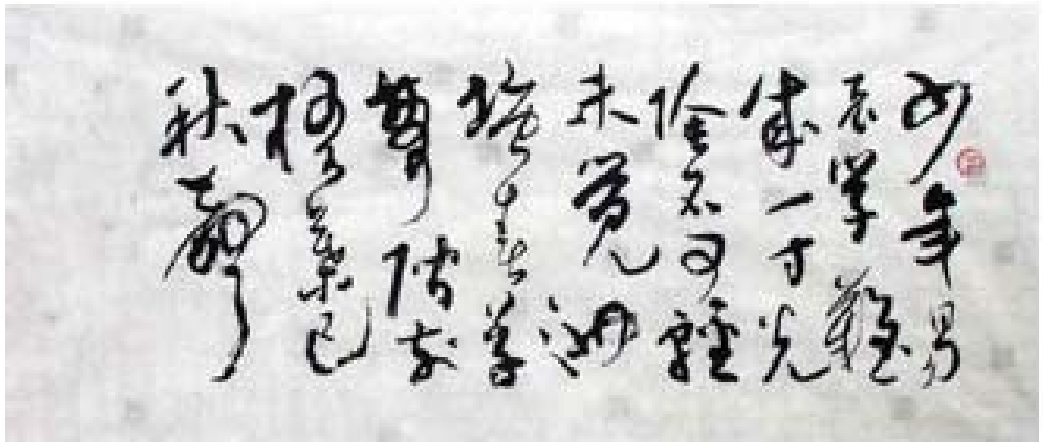
How to Send with Digital Signature?







How to Receive Digital Signature?



&

How to Receive Digital Signature?

If a = b, then the message has been transmitted correctly.

If a ≠ b, then an error occurred! The message has been modified!

Why do we need Digital Signature?

Without Digital Signature,

The calligraph could be sent by anybody.

With Digital Signature,

The calligraph is really sent by Dave.

A Digital Signature accomplishes 2 jobs for us:

1. Proves the data integrity of the message is intact.
2. The person who sent the message really is who you think he is.

Man-in-the-middle Attack

• Designed to intercept the transmission of a public key or to even insert a known key structure in place of the requested public key.

• Attackers attempt to place themselves between the sender and receiver, intercepting the request for key exchanges. the attacker sends each participant a valid public key.

• Attacker receives each encrypted message and decodes it within the key given to the sending party.

• The decoded message is then encrypted and sent to the originally intended recipient.

Remember!!!

A Digital Signature is NOT a scan of a signature!

------ David Yang

(Feel free to quote)

THANK YOU

Created by DAVID YANG