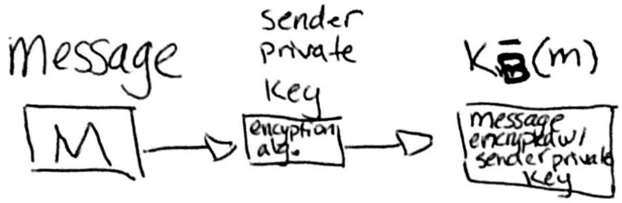
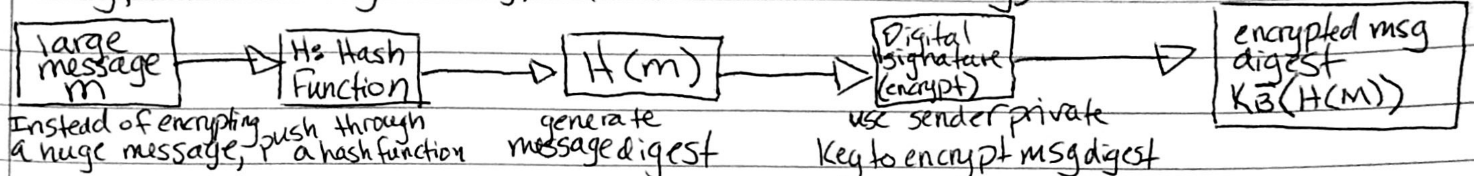


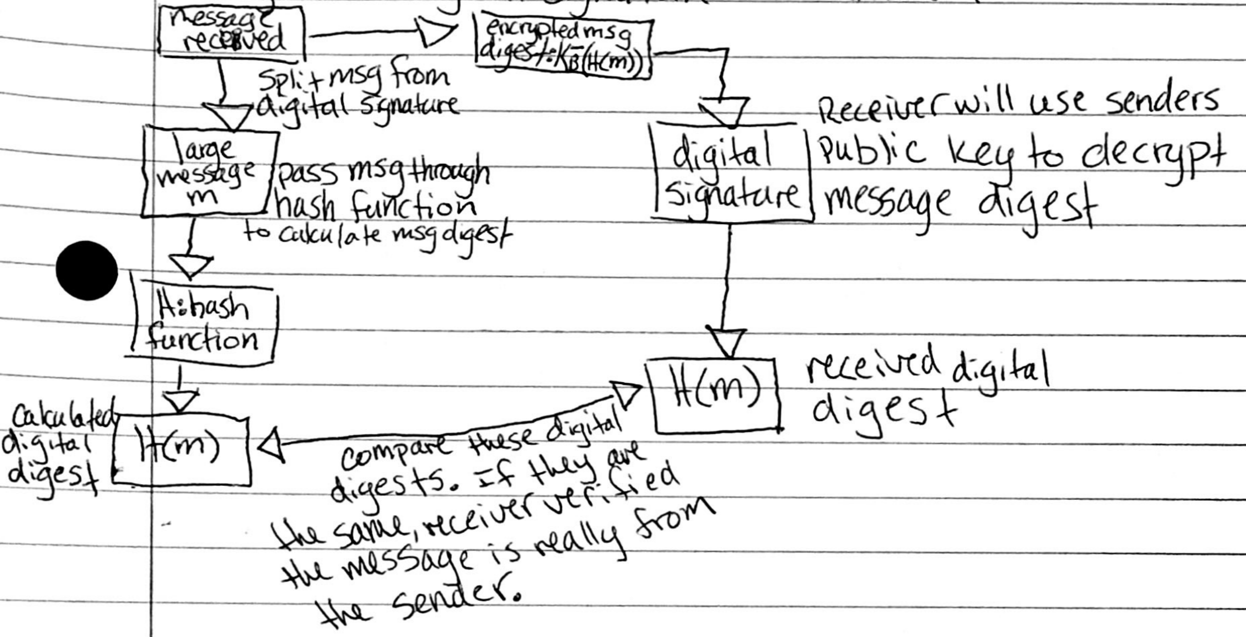
8) Digital signature: Similar to MAC or a handwritten signature.

For MAC → Can only verify message integrity — NOT Sender ID.

W/ Digital signature, sender ID can be verified w/ privat(unique) Key. Private key signs the message and receiver can prove it's from who it should be by using the sender's public key to decrypt the message (encrypted w/ sender private key).


large message m
H: Hash Function
H(m)
Digital signature (encrypt)
encrypted msg digest $K_B^-(H(M))$
Instead of encrypting a huge message, push through a hash function
generate message digest
use sender private key to encrypt msg digest

— message and digital signature are sent out —


message received
encrypted msg digest: $K_B^-(H(m))$
Split msg from digital signature
large message m
pass msg through hash function to calculate msg digest
digital signature
Receiver will use senders public key to decrypt message digest
$(K_B^+(H(m)))$
H: hash function
H(m)
received digital digest
Calculated digital digest
H(m)
compare these digital digests. If they are the same, receiver verified the message is really from the sender.

9) The above diagrams also show how a digital signature is verified. The sender encrypts the message or message digest with the private key. When the receiver gets the message, they are able to decrypt it using the sender's public key. This ensures nobody else could have encrypted it.

10) A certification authority binds a public key to some entity (entity = e) (as a drivers license does). CA is a database, tracking entities to public keys (i.e., Amy = P_B^+, Bob = P_B^+). Entities register public key to CA, proving its identity. CA then creates a certificate binding key to e. Certificate with e's public key is digitally signed w/ CA's private key. With this, users/receivers know the sender/site can be trusted.