Hashes, MACs and Authenticated Encryption

- So far: Symmetric encryption works if particpants share a key
- Public key cryptography and key distribution protocols ensure that key is shared and safe
- Still need to detect manipulation of ciphertext
- Hashes, MACs and Authenticated Encryption address this

Hashes

- A hash of any message is a short string generated from that message.
- The hash of a message is always the same.
- Any small change makes the hash totally different.
- It is very hard to go from the hash to the message.
- It is very unlikely that any two different messages have the same hash.

Uses of Hashing

- Verification of download of message
- Tying parts of a message together (hash the whole message)
- Hash the message, then sign the hash (for electronic signatures)
- Protect passwords
    - Store the hash, not the passwords

Attacks on hashes

- *Preimage attack:* Find a message for a given hash: very hard.
- *Collision attack:* Find two messages with the same hash.
- *Prefix collision attack:* A collision attack where the attacker can pick a prefix for the message.

Birthday paradox

- How many people do you need to ask before you find two people that have the same birthday with probability 0.5?

Birthday paradox

- How many people do you need to ask before you find two people that have the same birthday with probability 0.5?
- 23 people, gives $\frac{23*22}{2} = 253$ pairs
- Probability that two people have a different birthday is $364/365$.
- The probablility is $(\frac{364}{365})^{253} = 0.4995$

The SHA Family of Hashes

- The most common (and best) hashes are the SHA (Secure Hash Algorithm) hashes.
- 1993, The US National Institute of Standards and Technology (NIST), developed a new hash SHA-0
- 1995, the NSA stepped in and fixed it: SHA-1 (160-bit hash).

SHA1

- A birthday attack on SHA-1 should need 2^{80} hash tests
- In 2005 a 2^{63} attack was found.
- Not really practical, but no-one trusts SHA-1 any more.
- So $\cdots$ SHA-2

SHA2

- SHA2 is an improved version of SHA1 with a longer hash.
- 256 or 512 bits: also called SHA256, SHA512.
- Based on SHA-1 it has some of the same weaknesses. So, even though it seems secure the cryptographers aren't happy.

The SHA-3 Competition

- Submissions opened on October 31, 2008,
- Round 1
    - 13 submissions rejected without comment. 10 withdrawn by authors. 16 rejected for design or performance.
    - Including Sony's
- Conference in Feb 2009. 14 scheme picked to go through to round 2.

  Dropped Schemes include
    - Ron Rivest's,
    - Lockheed Martin

The SHA-3 Competition

- Winner announced on October 2, 2012 as Keccak, (Daemen et al. the AES guy)
- Adopted as NIST-standard in 2015

Merkle–Damgård (MD) Hashes

- The MD family of hashes is also popular.
- MD4 and MD5 used, but weak.
  - Only useful when we only care about preimage attacks or Integrity.
- MD6: Ron Rivest's candidate for SHA3.
  - Seems good and fast.

Examples of hashes

- md5
- shasum
- shasum -a 512

Message Authentication Codes

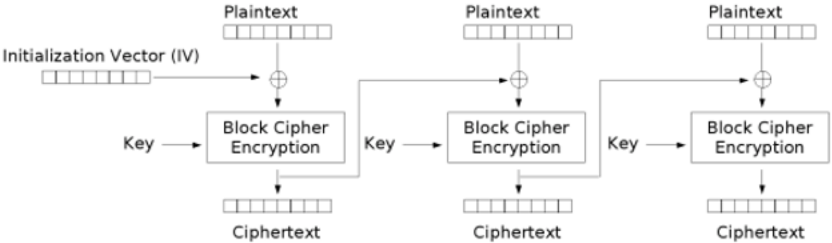
- Abbreviated often as “MAC”, has nothing to do with MAC in MAC address for networking (MAC = Media Access Control)
- MACs sometimes used for authentication:
  - Example: Alice and Bank share key k, Alice sends to bank

$$\text{"Pay Bob £10"}, MAC_k(\text{"Pay Bob £10"})$$

- Possible attack on MAC: Add data to a MAC without knowing the key (Length extension attack)

How can we make a MAC?

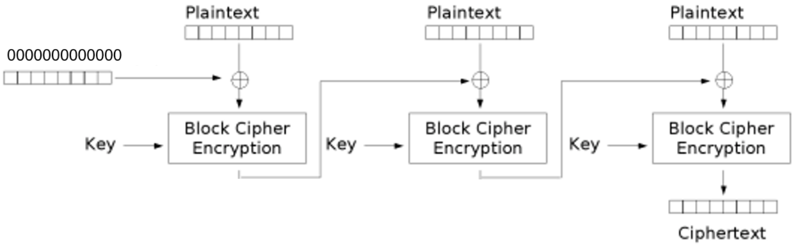
Block Cipher Modes



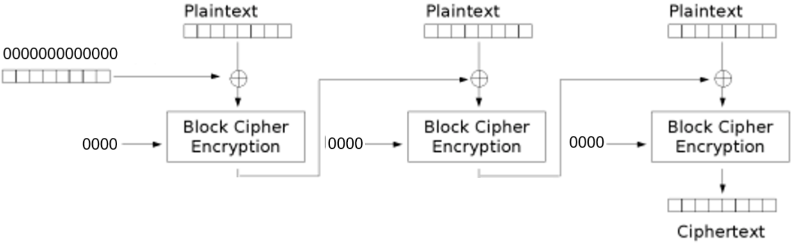
Cipher Block Chaining (CBC) mode encryption

Source: Wikipedia

Making a CBC MAC



An Inefficient Hash Function



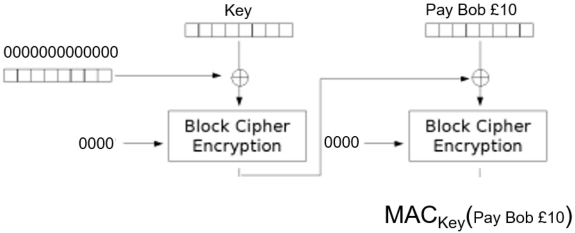
Broken Hash to MAC

- If we had a Hash we could try to make a MAC by:

$$MAC_{Key}(M) = H(Key, M)$$

- But this might allow a length extension attack.

Broken Hash to MAC



Cipher Texts Can Be Altered

- AES encryption with a particular key maps any 128-bit block to a 128-bit block (or 256)
- AES decrypt also maps any 128-bit block to a 128-bit block.
- Decrypt can be run on any block (not just encryptions).

Block mode

- CBC mode: any change affects all of the rest of the message.
- ECB mode: any change affects only the block.
- CTR mode: any change affects only the bits altered.

Known Plain Text Attacks

- If I know the plaintext I can change CTR encrypted messages. (see previous lecture)

Authenticated Encryption Modes

- Authenticated encryption modes stop this.
- With Authenticated Encryption you can only form a valid ciphertext if you know the key.
- Most common way to do this is to add a MAC to the ciphertext.

CCM mode encryption

- First calculate an AES CBC-MAC on the data.
- Then encrypt the message followed by the MAC using the same key and CTR mode.
- Not rocket science, but proven secure
  - Fully defined as RFC 3610

Summary

Defined ways of detecting manipulation of ciphertexts

- **Hashes**: Detect corruption of messages in general. New hashes can be generated by the attacker
- **MAC (Message Authentication Codes)**: use a key to ensure that message has not been changed
- **Authenticated Encryption**: provides encryption such that manipulation of cipher texts can be detected. Often uses MACs.