Boardplan: message authentication (5/2/06)

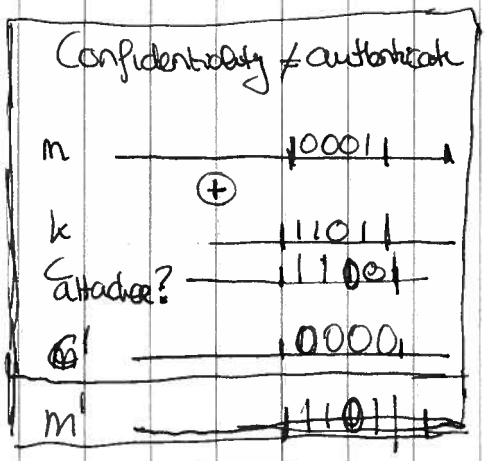
Slides

→ last few boards from conf.

① Outline
- Wrap Confidentiality
- Authentication

→ One-time pad
XOR.
+
RC4.

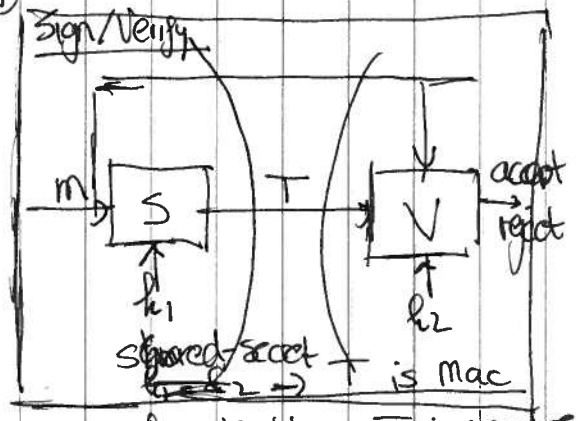
② Confidentiality ≠ authenticity



③ Solutions
- ✗ checksum ✗
  - should also work unencrypted
- ✗ ~~key dependent checksum~~
  cryptographic checksum.
  $H(m) = V$ s.t.
  $H(m) \Rightarrow m$
  $H(m') \neq H(m)$
- ⇒ key dependent one

@ Auth + Conf.
sign(encrypt(M, k_E)K_S).

④ Sign/Verify



→ public key ⇒ T is signature.

⑤ Attacks © crypto.
1. Modify m
2. Reorder m
3. Extend m
4. Splice m.

⇒ H(m + key) not good enough.

⑤a slide w. hmac

⑥ key distribution problem
- A → B: "here is my auth key k"
- ?
- → physical rendezvous
- →

⑦ slide w. public key ⑧ RSA. slides + sign + verify.