Collision resistance

Timing attacks on MAC verification

verification timing attacks [L’09]

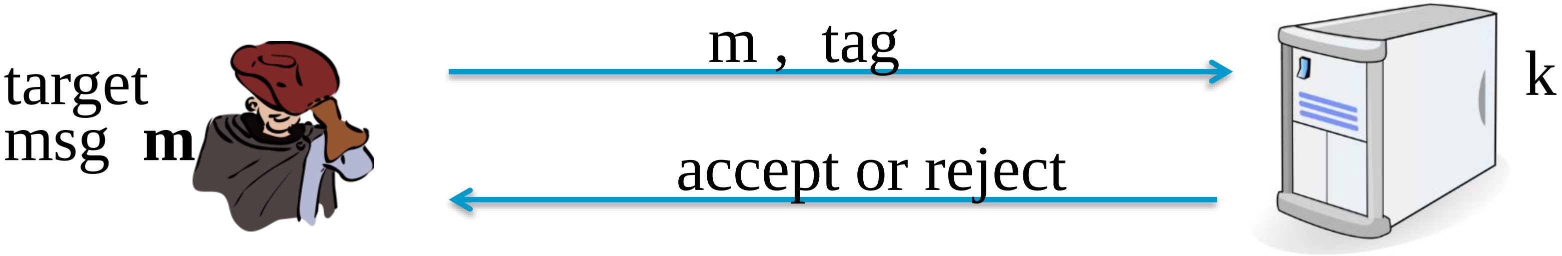
Example: Keyczar crypto library (Python)
[simplified]

```
def Verify(key, msg, sig_bytes):
    return HMAC(key, msg) == sig_bytes
```

The problem: ‘==‘ implemented as a byte-by-byte comparison

- Comparator returns false when first inequality found

Warning: verification timing attacks [L'09]



target msg **m**

m , tag

accept or reject

k

Timing attack: to compute tag for target message m do:

Step 1: Query server with random tag

Step 2: Loop over all possible first bytes and query server.
stop when verification takes a little longer than in step1

Step 3: repeat for all tag bytes until valid tag found

3	53	*	*	*	*

Assignment

- Towards the verification timing attacks, Pls propose your defense strategy and try to implement it.