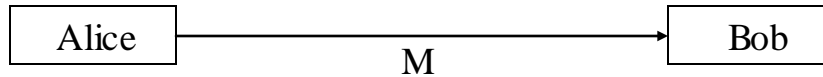


Network Security

Lecture Notes, October 2nd 2009

Message Integrity:



Alice sends a message m to Bob. Bob wants to know whether the message received is the correct message without any modifications to it. The message integrity is usually handled using Message Authentication Code (MAC).

Alice and Bob use a key 'K'.



$$t = F(k, m)$$

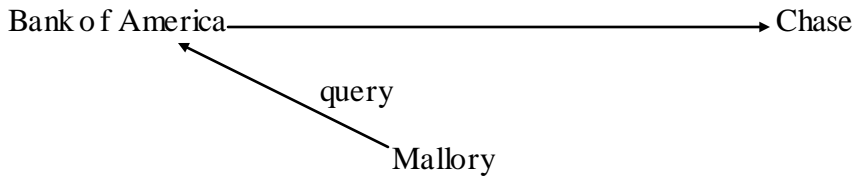
```
if (t' = F(k, m'))
    output m'
else
    output error.
```

MALLORY' GOALS:

- Modify m , and modify 't' to match.
- Compute tag for some message of her choice.
- Compute 'k'
- Find tag collision.
- Brute force guessing.

ATTACKER'S RESOURCES:

- Observe valid (m, t) pairs.
- Query MAC oracle.
- Query Verification Oracle.



Definition:

A MAC scheme is (t, q, q', ϵ) secure if for all A running in time $\leq t$ and making at most q MAC oracle queries and at most q' verification oracle queries,

$$|\Pr[A^{\text{MAC}_K, \text{Verf}_K} \text{ for ges}]| \leq \epsilon$$

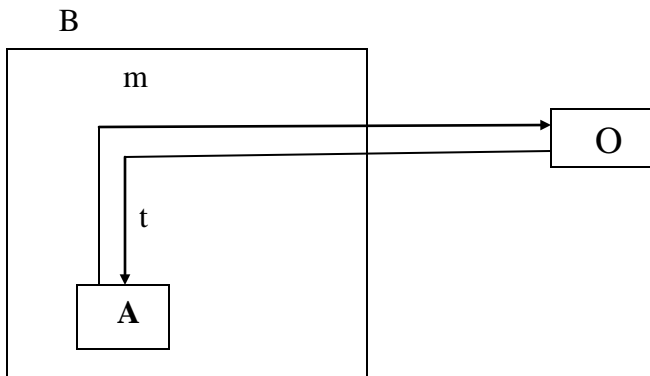
where A for ges if A queries verf_k on (m, t) and $\text{verf}_k(m, t) = \text{OK}$ and A has not previously queried MAC_k on M .

Theorem:

If $F: \text{keys} * \{0,1\}^l \longrightarrow \{0, 1\}^{2l}$ is a (t, q, ϵ) secure PRF, then:

F is a $(t - O(q), q', q - q', \epsilon + (q - q')/2^l)$ MAC.

Proof: (By Contrapositive)



If $O = R$, then $\Pr[A \text{ forges}] = (q-q') / 2^l$. i.e $\Pr[B^0 = 1] = 2^{-l}$.

If $O = F_k$, then $\Pr [A \text{ forges}] \geq \epsilon + ((q - q') / 2^l)$ by the assumption that A breaks F_k as a MAC.

Therefore,

$$|\Pr [B^R = 1] - \Pr[B_k^F = 1]| \geq \epsilon.$$

Hence, A PRF is a MAC.