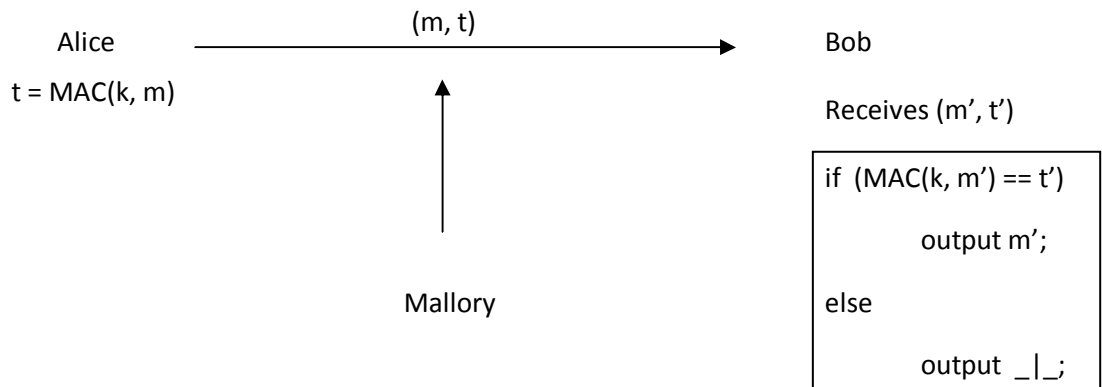


## Network Security

Sumeet P Dash

October 2, 2009

### Message Integrity:



[MAC = Message Authentication Code]

### Mallory Goals:

- Modify  $m$  and then modify  $t$  correspondingly to reflect the change.
- Compute tag for some message of her choosing.
- Find and exploit tag collision.
- Compute the value of key  $(k)$ .

### Attacker's Resources:

- Can observe  $(m, t)$  pairs over a period of time.
- Query MAC oracle (to find out the tag for a message of her choosing).
- Query verification oracle (To check whether his computed value of MAC is right).

### Definition of a secure MAC scheme:

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

$$\Pr [A^{\text{MAC}_k, \text{Verf}_k} \text{ forges}] \leq \epsilon$$

where A forges if A queries  $\text{Verf}_k$  on  $(m, t)$  and  $\text{Verf}_k(m, t) = \text{OK}$  and A has not previously queried  $\text{MAC}_k$  on  $m$ .

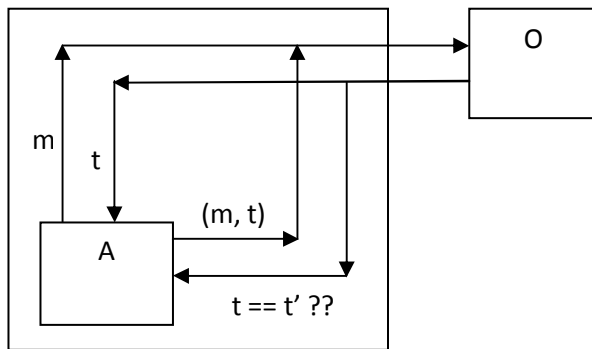
**Theorem:**

If  $F: \text{key} \times \{0, 1\}^* \rightarrow \{0, 1\}^l$  is a  $(t, q, \epsilon)$  secure PRF, then  $F$  is a  $(t - O(q), q', q - q', \epsilon + (q - q')/2^l)$  secure MAC.

**Proof (By Contrapositive):**

Let's assume that  $F$  is not secure as a MAC, i.e. A breaks  $F$  as a MAC.

**B**



Output of B is 1 if A forges.

If  $O = R$ , then  $\Pr[A \text{ forges}] = 2^{-l}$

i.e.  $\Pr[B^R = 1] = 2^{-l}$

$\Pr[A \text{ forges}] = 2^{-l}$  if A makes 1 query and

$\Pr[A \text{ forges}] = (q - q')/2^l$  if A gets to make  $(q - q')$  queries.

Now,

if  $O = F_k$ , then  $\Pr[A \text{ forges}] \geq \epsilon + (q - q')/2^l$

by assumption that A breaks  $F_k$  as a MAC.

i.e.  $\Pr[B^{F_k} = 1] \geq \epsilon + (q - q')/2^l$

Therefore,  $|\Pr[B^R = 1] - \Pr[B^{F_k} = 1]| \geq \epsilon$  which is against the standard definition of  $F_k$ . Hence proved.