Introduction to Cryptography CS 355

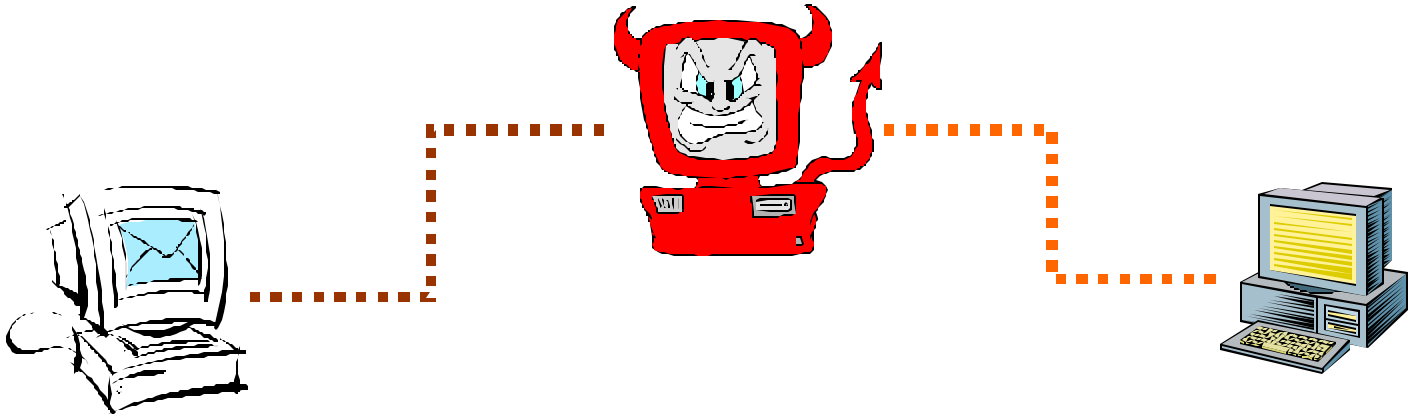
Lecture 28

Message Authentication Code

Lecture Outline

- Message Authentication Code (MAC)
- Security properties of MAC

Data Integrity and Source Authentication



- Encryption does not protect data from modification by another party.
- Need a way to ensure that data arrives at destination in its original form as sent by the sender and it is coming from an authenticated source.

Limitation of Using Hash Functions for Authentication

- Require an authentic channel to transmit the hash of a message
  - anyone can compute the hash value of a message, as the hash function is public
  - not always possible
- How to address this?
  - use more than one hash functions
  - use a key to select which one to use

Hash Family

- A hash family is a four-tuple (X, Y, K, H), where
  - X is a set of possible messages
  - Y is a finite set of possible message digests
  - K is the keyspace
  - For each $K \in K$, there is a hash function $h_K \in H$. Each $h_K: X \rightarrow Y$
- Alternatively, one can think of H as a function $K \times X \rightarrow Y$

Message Authentication Code

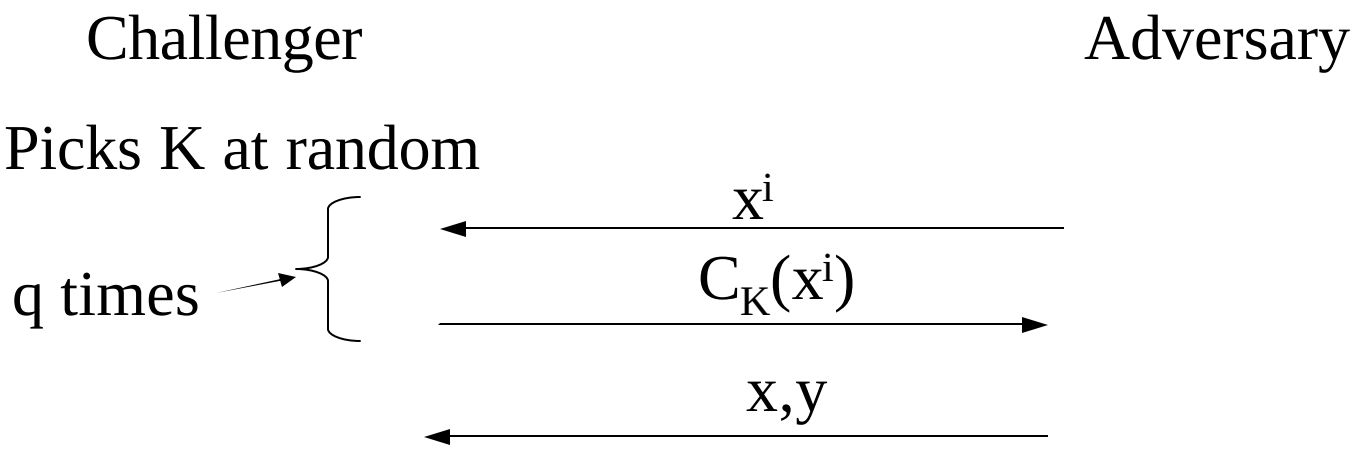
- A MAC scheme is a hash family, used for message authentication
- MAC = $C_K(M)$
- The sender and the receiver share K
- The sender sends (M, $C_k(M)$)
- The receiver receives (X,Y) and verifies that $C_K(X)=Y$, if so, then accepts the message as from the sender
- To be secure, an adversary shouldn't be able to come up with (X,Y) such that $C_K(X)=Y$.

Constructing MAC from Hash Functions

- Given a cryptographic (iterative) hash function h,
- Define $C_K(M)$ to be h(M) with K as IV
- Is this secure?
- Given a message x and its MAC $C_K(x)$, the adversary can construct x' and $C_K(x')$
  - let pad(x) be the padding added to x
  - let x'=x || pad(x) || w, y'=x' || pad(x')
  - then $C_K(x')$ can be computed from $C_K(x)$

Existential Forgery Attack against MAC

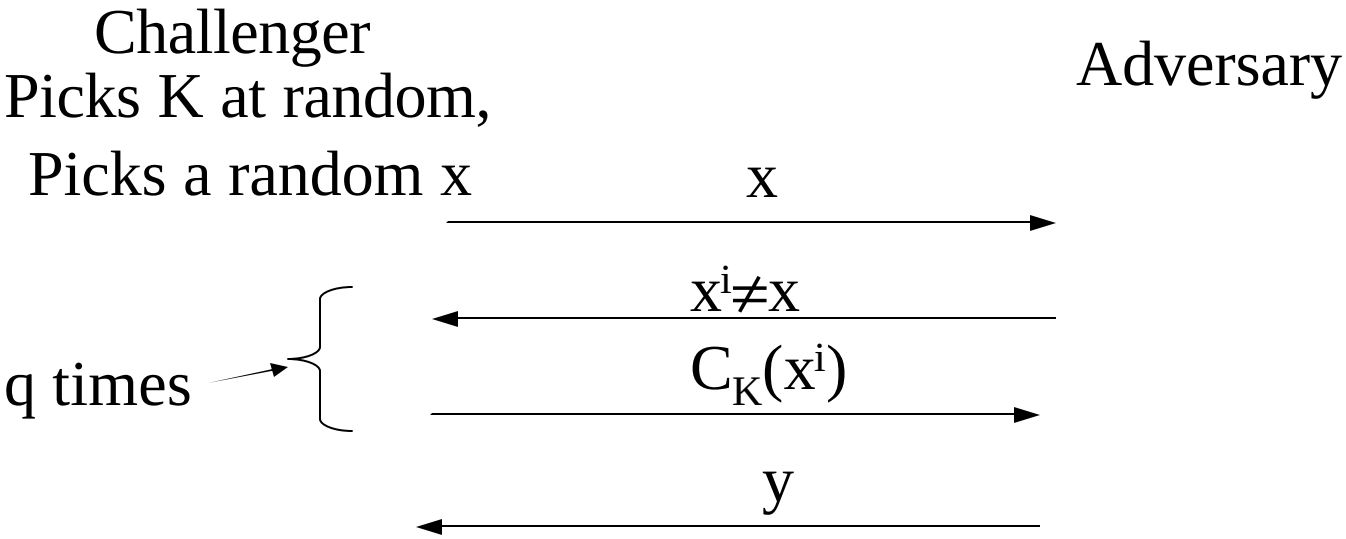
- Let C be a MAC function $C_K(M)$ is the MAC for M under K.



Attacker wins game if $x \notin \{x^1,\ldots,x^q\}$ and $C_K(x)=y$

Selective Forgery Attack Against MAC

- Let C be a MAC function $C_K(M)$ is the MAC for M under K.



Attacker wins game if and $C_K(x)=y$

MAC Security

- The pair (x, z) is called a forgery
- A (ε,q) forger
  - can produce a forgery with probability ε, after making q queries
  - generally talks about existential forgery

- The attacker against the MAC scheme $C_K(M)=h(M)$ with K as IV is a (1,1) forger

Constructing MAC using Hash Functions

- Are the following MAC schemes secure? What kind of forgers exist for them?
  - $C_K(M) = h(K \,||\, M)$, where h is a cryptographic hash function

Coming Attractions …

- HMAC
- CBC-MAC