Review :

Proof of security of CBCMAC out of syllabus

- Message Authentication Codes (MAC)
- Security Definition → CBCMAC

Simple MAC Construction & Proof of Security

For an n bit message $F_k : \{0,1\}^n \to \{0,1\}^n$

tag = $MAC_k(m) = F_k(m)$

For an arbitrarily long string, we want $MAC_k : \{0,1\}^* \to \{0,1\}^*$

since this works for $t=1$ in $m = m_1 m_2 \ldots m_t$

where $|m_i| = n$ bits

Attempt 1 :

$t_i = F_k(m_i)$, $t = t_1 t_2 \ldots t_t$

Flawed - Susceptible to permuting attack, can get tag for a permutation of $m_1 m_2 \ldots m_t$ without querying

Patch : $t_i = F_k(i \| m_i)$, $|m_i| = n/2$

Not susceptible to permutation attack, each tag has a sequence attack

Flawed : Interleaving Attack

$m_1 m_2 \ldots m_{t_1}$

$m_1' m_2' \ldots m_{t_2}'$

$m_1 m_2' m_3 m_4' \ldots$ → can get tag

Flawed : Prefix attack : can get tag for any prefix, though not queried

Patch for prefix attack : add length of message. $t_i = F_k(\ell \| i \| m_i)$ $|m_i| = n/3$

Still susceptible to interleaving attack

(These are the only 3 attacks on MACs)

Patch for interleaving attack :

$t_i = F_k(r \| \ell \| i \| m_i)$ $|m_i| = n/4$

↳ random nonce, used as message id

$t = r \| t_1 \| t_2 \ldots \| t_t$

Q - Set of all queries to MAC_k server

If MAC_k is secure,

$Pr[\,Vrfy(m,t)=1 , \exists\, m \notin Q\,] \le negl(n)$

r used by adv. in m

is new

Pr of success $\le 2^{-n}$

occurs in Q

unique

many occurs with prob $\le 2^{-n}$

If r occurred once in Q,

Let $m' \in Q$, $t' = r \| t_1' \| t_2' \| \ldots$

If $|m'| = |m|$ or $|m'| \neq |m|$

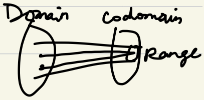
↳ $t_i = F_k(r \| \ell \| i \| m_i)$

Prob $\le 2^{-n}$

$\not\ni$ If $|m'| = |m|$, $\exists i \ni m_i' \neq m_i$

So prob of predicting tag $t_i = 2^{-n}$

Hashing



Want Collision-Resistance

Collision : $x \neq y$, $H(x) = H(y)$

Family of hash function → choose 1 uniformly at random & provide to adversary

$H^s : \{0,1\}^* \rightarrow \{0,1\}^n$

superscript because not private indexing

Security parameter = length of indexer

Probability is over the diff. hash fns in the family

Is said to be collision resistant if $\forall$PPTM A

$P(A(s) = (x,y) \ni x \neq y, H^s(x) = H^s(y)) \leq negl(|s|)$

Generic Birthday Attack :

What is the min. no. of people in a room

$\ni$ Pr [At least 2 people have same birthday] ≥ 0.5

: 23

Next Up: Generic Birthday Attack, Merkle-Damgard Transform, Provably secure hashing, HMAC

Use for tamper resistance, security vs performance