AES-EMAC

\[ \text{MAC}(K, M) = T \quad M = P_1 || \ldots || P_n \]

Consider \( H(M) = \text{MAC}(K, M) \)

\[ P_1 || P_2 \ldots || P_n \rightarrow T \]

\[ (S_1 \oplus P_2) \rightarrow T = P_n \rightarrow T \]
HMAC is both a MAC and collision resistant when the attacker has key K.

\[
\text{HMAC}(K, M) = H\left( K \oplus \text{pad} \| H(K \oplus \text{ipad} \| M) \right)
\]

Assume \( H \) is a collision resistant hash 0x5c...5c 0x36...3c

Why collision resistant? Because \( H \) is CR

Assume \( H(\text{HMAC}(K, M_1)) = \text{HMAC}(K, M_2) \)

\[
\Rightarrow K \oplus \text{pad} \| H(K \oplus \text{ipad} \| M_1) =
\]

\[
= K \oplus \text{pad} \| H(K \oplus \text{ipad} \| M_2)
\]

\[
\Rightarrow K \oplus \text{ipad} \| M_1 = K \oplus \text{ipad} \| M_2
\]

\[
\Rightarrow M_1 = M_2
\]
Digital signatures

Alice: \[ M, \text{sign}(SK_A, M) = \text{sig} \] \rightarrow Bob

SK_A, PK_A

integrity & authenticity in the asymmetric setting

Syntax:
- \text{Keygen}() \rightarrow SK, PK
- \text{Sign}(SK, M) \rightarrow \text{sig}
- \text{Verify}(PK, m, \text{sig}) \rightarrow 0 \text{ or } 1

Correctness: \[ \forall m, SK, PK \]
\[ \text{Verify}(PK, m, \text{sign}(SK, M)) = 1 \checkmark \]
Security: EU-CPA

existential unforgeable under CPA...

\[ \text{Ch} \quad (\text{PK}) \quad \text{everyone knows it} \quad (\text{Adv}) \]

\[ \text{SK}_{\text{PK}} \quad \leftarrow \quad M_i \quad \text{Sign}(\text{SK}, M_i) \quad \rightarrow \quad Q \]

\[ M_i^* \quad \text{Sign} \]

\[ \# \]

\[ \{ M_i \} \]

(Adv wins if \( M_i^* \neq \{ M_i \} \) and \( \text{Verify}(\text{PK}, M_i^*, \text{Sign}) = \text{yes} \))

\[ \Pr [\text{Adv wins}] \leq \text{negl} \]
RSA Signature

\textbf{Keygen()}: pick two random primes \( p \) and \( q \) of 2048 bits (both \( 2 \text{ mod } 3 \))
\[ n = pq = PK = n \]
\( \phi(n) = \text{Euler's totient function} \]
\( = \# \text{ of integers } \geq 0 \text{ that are } \gcd(\cdot, n) = 1 \)
\( \phi(n) = (p-1)(q-1) \text{ order of group modulo } n \)

\( \forall a, a^{\phi(n)} \equiv 1 \text{ mod } n \)

Compute \( d \) s.t. \( 3d \equiv 1 \text{ mod } \phi(n) \)

\( SK = d \)

\[ \exists r \text{ s.t.} \quad 3d = r \cdot \phi(n) + 1 \]
\[ \text{Sign} (SK, m) = \left( \frac{\text{hash}(m)^d}{H} \right) \mod n \]

\[ \text{Verify (PK, m, Sig)} : \quad \text{Sig}^3 \mod n = H(m) \mod n \]

Correctness:
\[ \left( \text{hash}(m)^d \right)^3 \mod n = \text{hash}(m) \mod n \]
\[ = \text{hash}(m)^{3d} \mod n \]
\[ = \text{hash}(m)^{\frac{1}{\phi(n)+1}} \cdot \text{hash}(m) \mod n \]
\[ = \text{hash}(m) \mod n \]
\[ \text{sign} (sk, m) = \frac{m^d \mod n}{\text{sig}} \]

How can you forge?

Signature for 1 is 1
for 0 is 0

\[ \text{sign} (sk, 1) = 1^d \mod n = 1 \]
\[ \text{sign} (sk, 0) = 0^d \mod n = 0 \]
Necessary assumption for security:
No Adv can factor large numbers.
Difficulty of factoring problem
If Adv could factor n
\[ n \rightarrow p, q \implies \phi(n) \implies d = SK \]