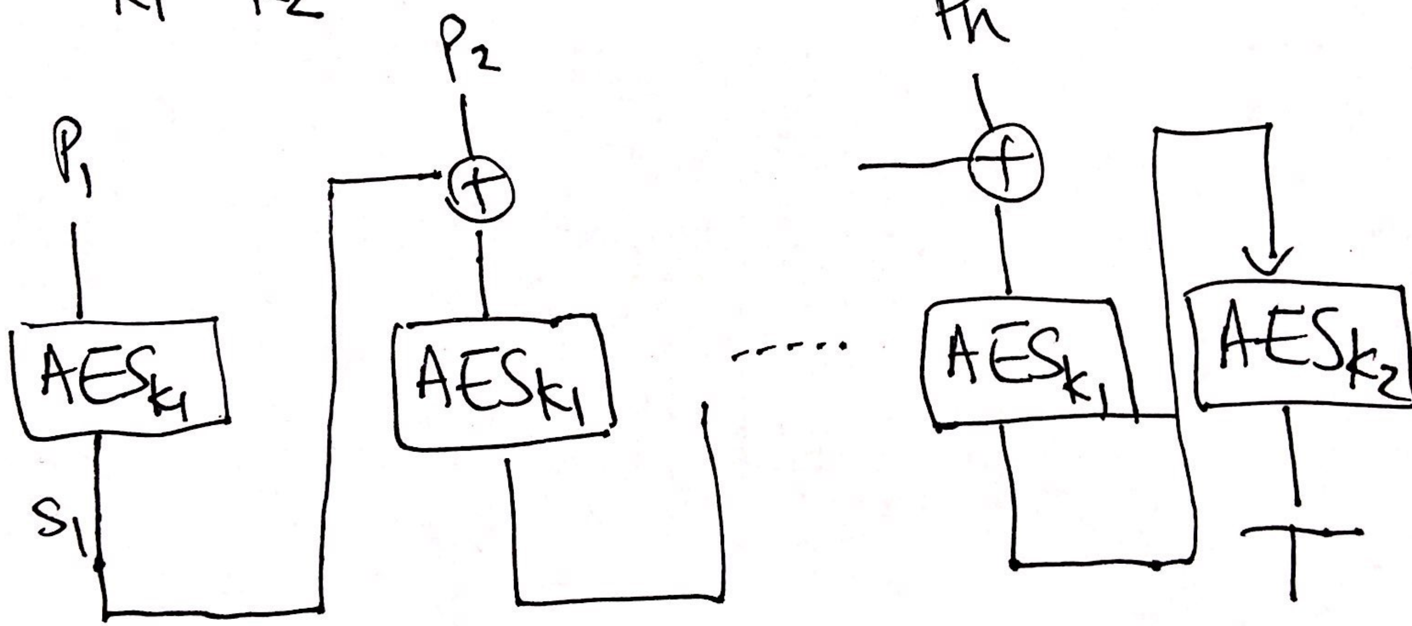
AES-EMAC

concat

$MAC(K, M) = T \quad M = P_1 \| \ldots \| P_n$

$K_1 \quad K_2$



Consider $H(M) = MAC(\check{K}, M)$ hash definition known to attacker

$P_1 \| P_2 \| \ldots P_n \to T$

$(S_1 \oplus P_2) \| \ldots P_n \to T$

HMAC both a MAC and collision resistant when the attacker has key K

$$HMAC(K, M) = H\Big(\underbrace{K \oplus opad}_{0x5C\ldots5C} \,\|\, H\big(\underbrace{K \oplus ipad}_{0x36\ldots36} \,\|\, M\big)\Big)$$

assume H is a collision resistant hash

Why collision resistant? Because H is CR

Assume $HMAC(K, M_1) = HMAC(K, M_2)$

$$\Rightarrow \cancel{K \oplus opad} \,\|\, H(K \oplus ipad \,\|\, M_1) = \cancel{K \oplus opad} \,\|\, H(K \oplus ipad \,\|\, M_2)$$

$$\Rightarrow K \oplus ipad \,\|\, M_1 = K \oplus ipad \,\|\, M_2$$

$$\Rightarrow M_1 = M_2$$

Digital signatures

$$\text{Alice} \xrightarrow{M,\ \text{sign}(SK_A, M) = \text{Sig}} \text{Bob}$$

SK_A, PK_A $\qquad\qquad$ SK_B, PK_B

$\text{Verify}(PK_A, M, \text{Sig}) = \checkmark$

integrity & authenticity in the asymmetric setting

Syntax:

$\text{Keygen}() \to SK, PK$

$\text{Sign}(SK, m) \to \text{Sig}$

$\text{Verify}(PK, m, \text{Sig}) \to 0/1$

Correctness: $\forall m, SK, PK$

$$\text{Verify}(PK, m, \text{Sign}(SK, m)) = 1 \checkmark$$

Security: EU-CPA

existential unforgeable under CPA ...

PK — everyone knows it

Ch		Adv
SK, PK	$\xleftarrow{\quad M_i \quad}$	
	$\xrightarrow{\ Sign(SK, M_i)\ }$	
	$\xleftarrow{\quad M', sig \quad}$	

$M' \notin \{M_i\}$

Adv wins if $M' \neq \{M_i\}$ and $Verify(PK, M', sig) = yes$

$\forall$ Adv

$Pr[\text{Adv wins}] \leq negl$

RSA Signature

$\boxed{\text{Keygen():}}$ pick two random primes p and q of 2048 bits (both 2 mod 3)

$n = p \cdot q \Rightarrow \boxed{PK = n}$

$\phi(n)$ = Euler's totient function
= # of integers ≥ 0 that are $\gcd(\cdot, n) = 1$

$\phi(n) = (p-1)\cdot(q-1)$ order of group modulo n

$\forall a,\ a^{\phi(n)} \equiv 1 \bmod n$

Compute d s.t. $\underbrace{3d \equiv 1 \bmod \phi(n)}$

$\Downarrow$

$\boxed{SK = d}$

$\exists r$ s.t.

$3d = r \cdot \phi(n) + 1$

$$\text{Sign}(\underset{\downarrow\, d}{SK}, m) = \underbrace{\text{hash}}_{H}(m)^{d} \bmod n$$

$$\text{Verify}(\underset{\downarrow\, n}{PK}, m, sig): \quad sig^{3} \bmod n \stackrel{?}{=} H(m) \bmod n$$

Correctness:

$$\left(\text{hash}(m)^{d}\right)^{3} \bmod n = \text{hash}(m)^{3d} \bmod n$$

$$= \text{hash}(m)^{r\cdot\phi(n)+1} \bmod n$$

$$= \left(\overset{1}{\cancel{\text{hash}(m)^{\phi(n)}}}\right)^{r} \cdot \text{hash}(m) \bmod n$$

$$= \text{hash}(m) \bmod n \quad \checkmark$$

$$\text{Sign}(SK, m) = \underbrace{m^d \bmod n}_{\text{sig}}$$

Insecure scheme.

How can you forge?

Signature for 1 is 1

for 0 is 0

$$\text{Sign}(SK, 1) = 1^d \bmod n = 1$$

$$\text{Sign}(SK, 0) = 0^d \bmod n = 0$$

Necessary assumption for security:

No Adv can factor large numbers.

Difficulty of factoring problem

If Adv could factor n

$n \Rightarrow p, q \Rightarrow \phi(n) \Rightarrow d = SK$