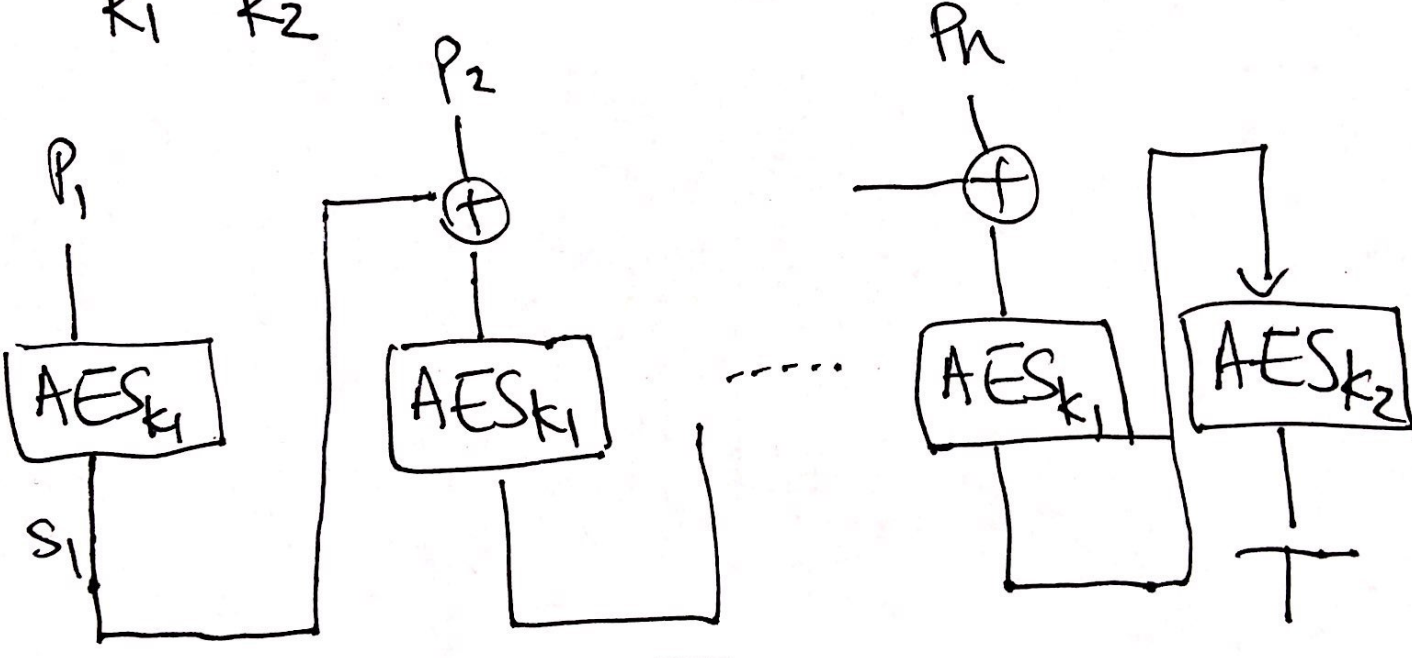
AES-EMAC

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

K_1 K_2



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

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

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

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

$$HMAC(K, M) = H\left(K \oplus opad \,||\, H(K \oplus ipad \,||\, M)\right)$$

assume H is a collision resistant hash

$0x5C...5C$ $0x36...36$

Why collision resistant? Because H is CR

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

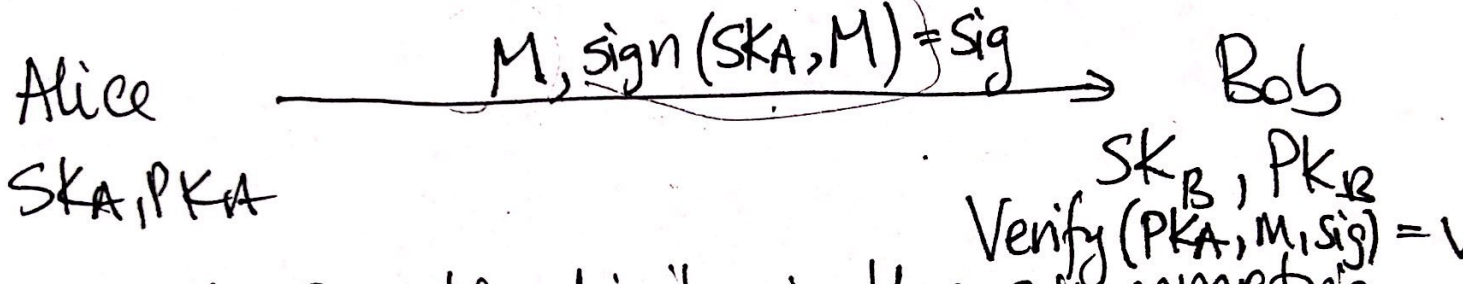
$\Rightarrow K \oplus opad \,||\, H(K \oplus ipad \,||\, M_1) =$

$= K \oplus opad \,||\, H(K \oplus ipad \,||\, M_2)$

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

$\Rightarrow M_1 = M_2$

Digital signatures



integrity & authenticity in the asymmetric setting

Syntax:

Keygen() → SK, PK

Sign(SK, m) → sig

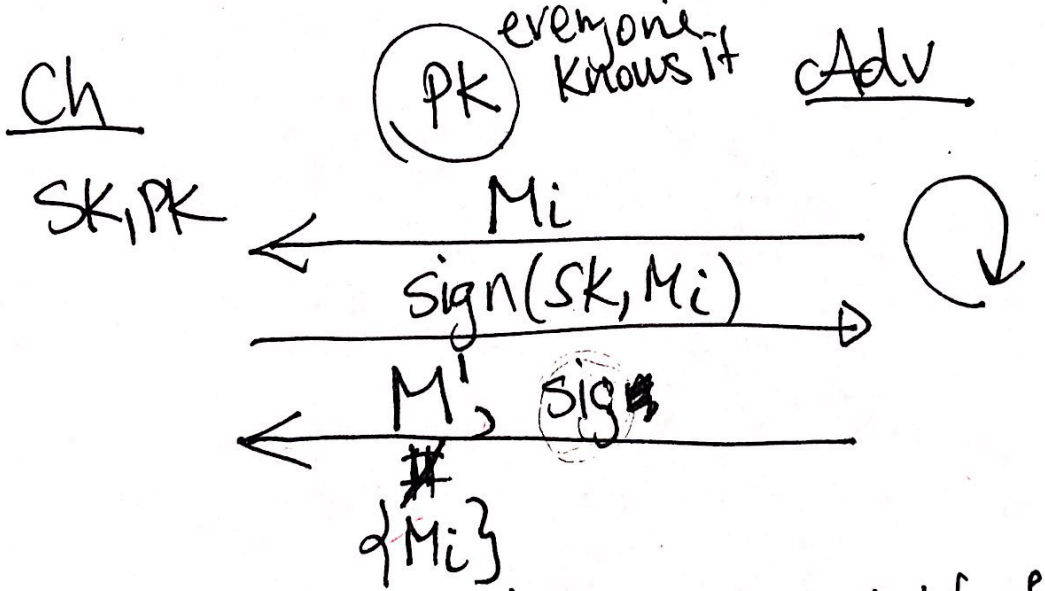
Verify(PK, m, sig) → 0/1

Correctness: ∀m, SK, PK

Verify(PK, m, Sign(SK, m)) = 1 ✓

Security: EU-CPA

existential unforgeable under CPA...



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

$\forall$ Adv

$Pr[Adv\ wins] \leq negl$

RSA Signature

Keygen(): pick two random primes p and q of 2048 bits (both 2 mod 3)

$n = pq$ $\Rightarrow$ **PK = n**

$\phi(n)$ = Euler's totient function

= # of integers ≥ 0 that are $\gcd(\cdot, n) = 1$

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

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

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

$\Downarrow$

$\exists r$ s.t.

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

SK = d

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

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

Correctness:

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

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

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

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

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

Insecure scheme.

How can you forge?

Signature for 1 is 1

for 0 is 0

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

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

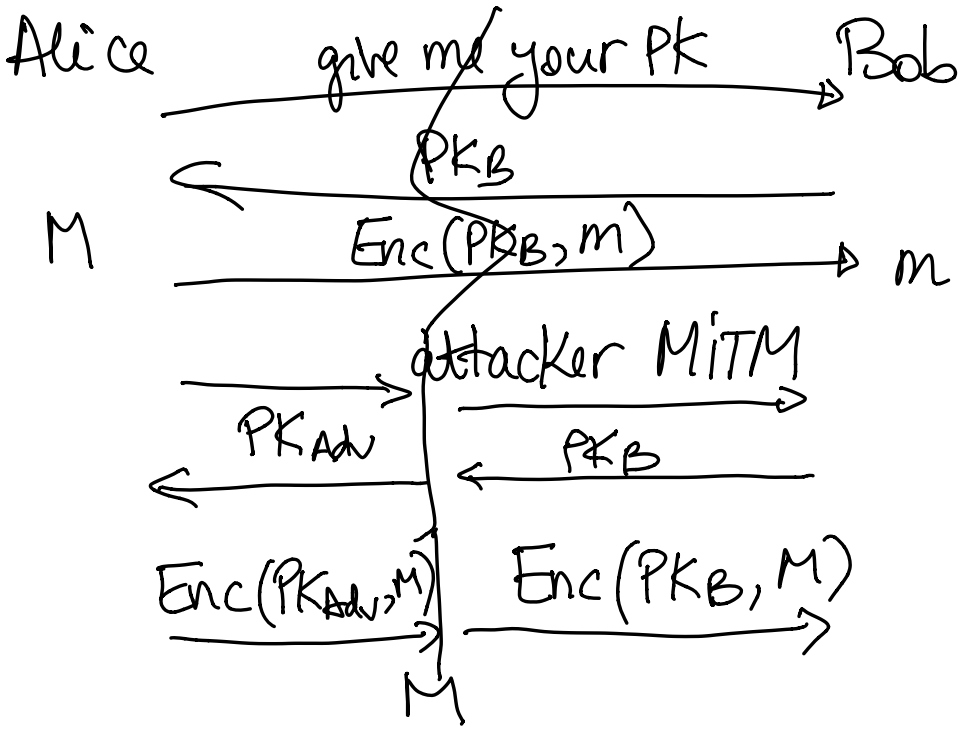
Necessary assumption for security:

- No Adv can factor large numbers.

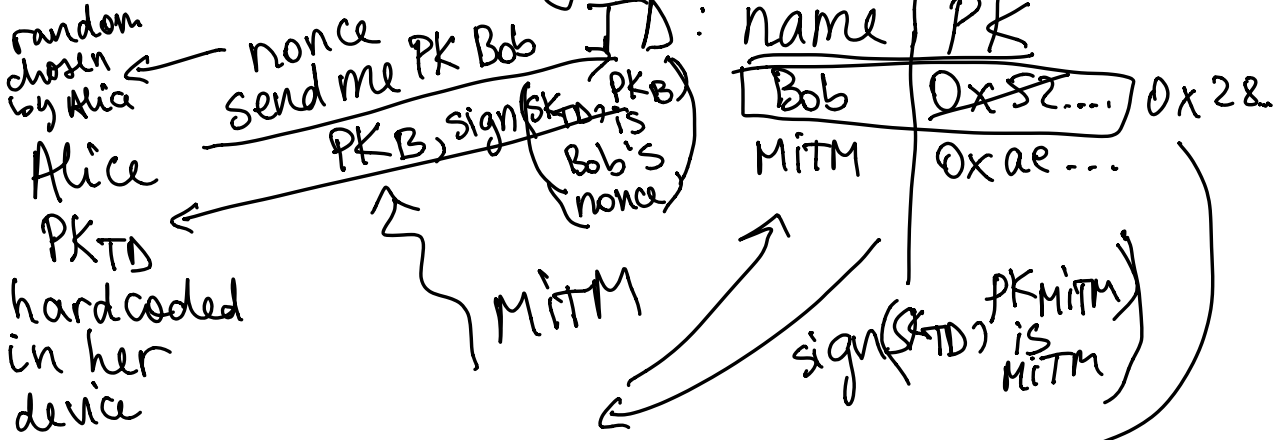
Difficulty of factoring problem

If Adv could factor n

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



Trusted directory



Updating a Key

Assume update happens securely

Replay attack:

Attacker replays old information (old sig with old PK)