RSA

p, q. $N = p \cdot q$, e, d (e: public, d: private)

Sign m → $s = m^d \bmod N$

Verify (m, s) $s = (H(m))^d \bmod N$

$m' = s^e \bmod N$

if $m' == M$ return true

else return false.

Alice
(d, N) // private

Only alice can sign

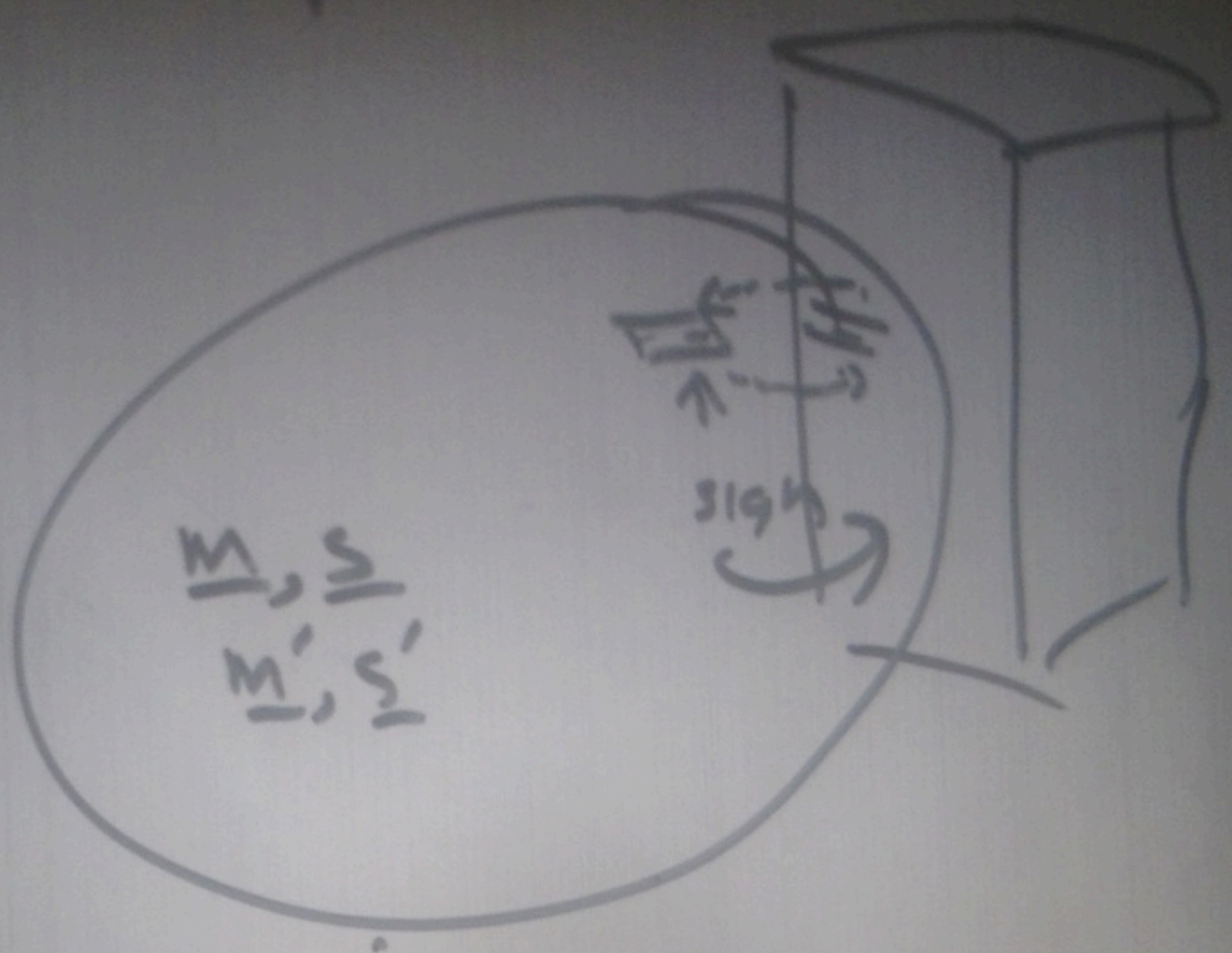
Bob
(e, N)
// public keys known

(m, s) →

Paul Kocher

VISA Cash.

Telephone



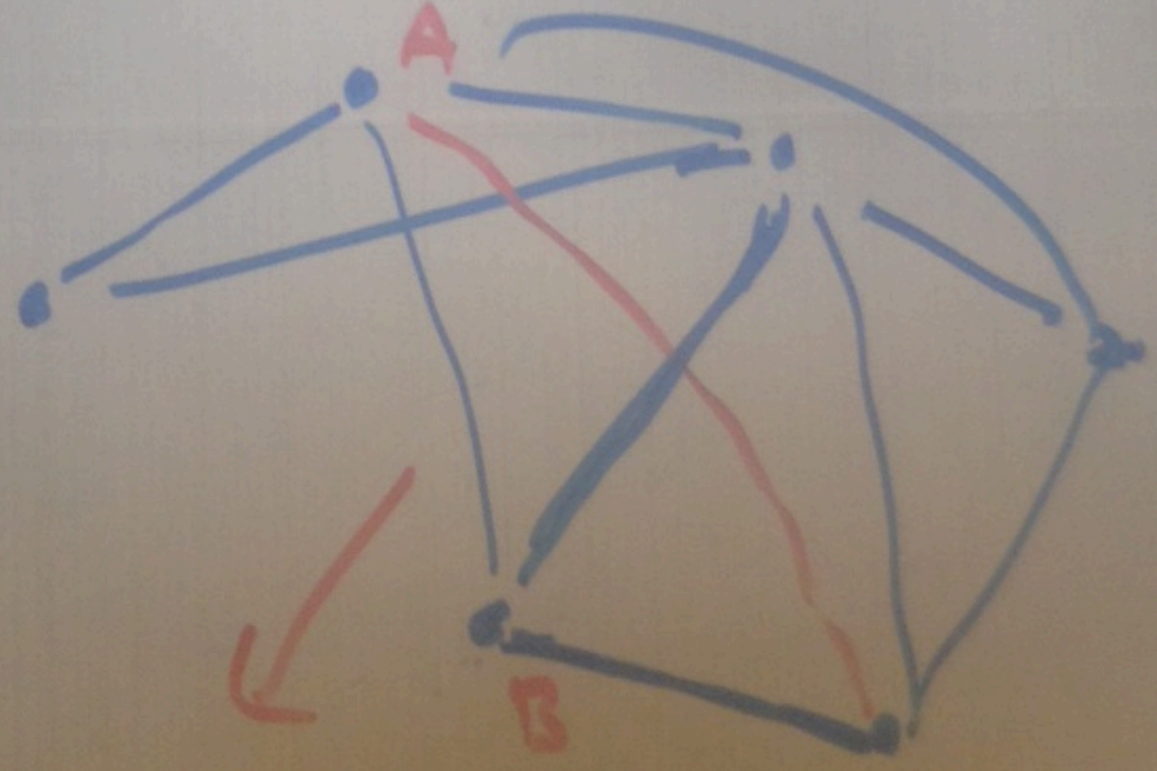
$sign_{(d,N)}(M.$

$(\#(M))^9 \bmod N.$

M=(Alice, public key, cannot be a CA)

M'(Alice, public key, CAN be a CA)

$H(M) = H(M')$ // H = MD5.

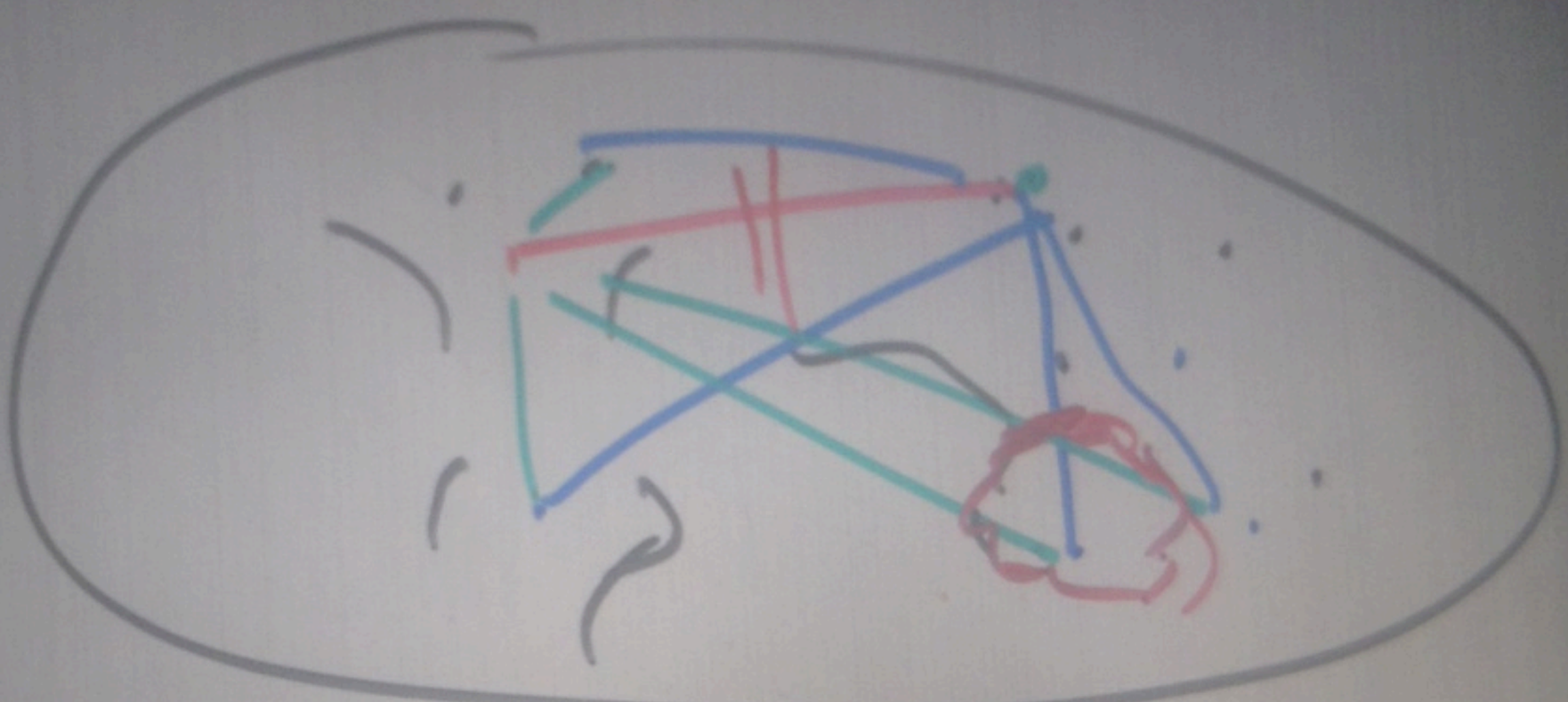


Bob signs "Bob believes PK_A belongs to Alice"

PGP

- 181 - RustCAs

Digital.



Symmetric

Enc
MAC → combine

AEAD

↳ authenticated encryption
associated data

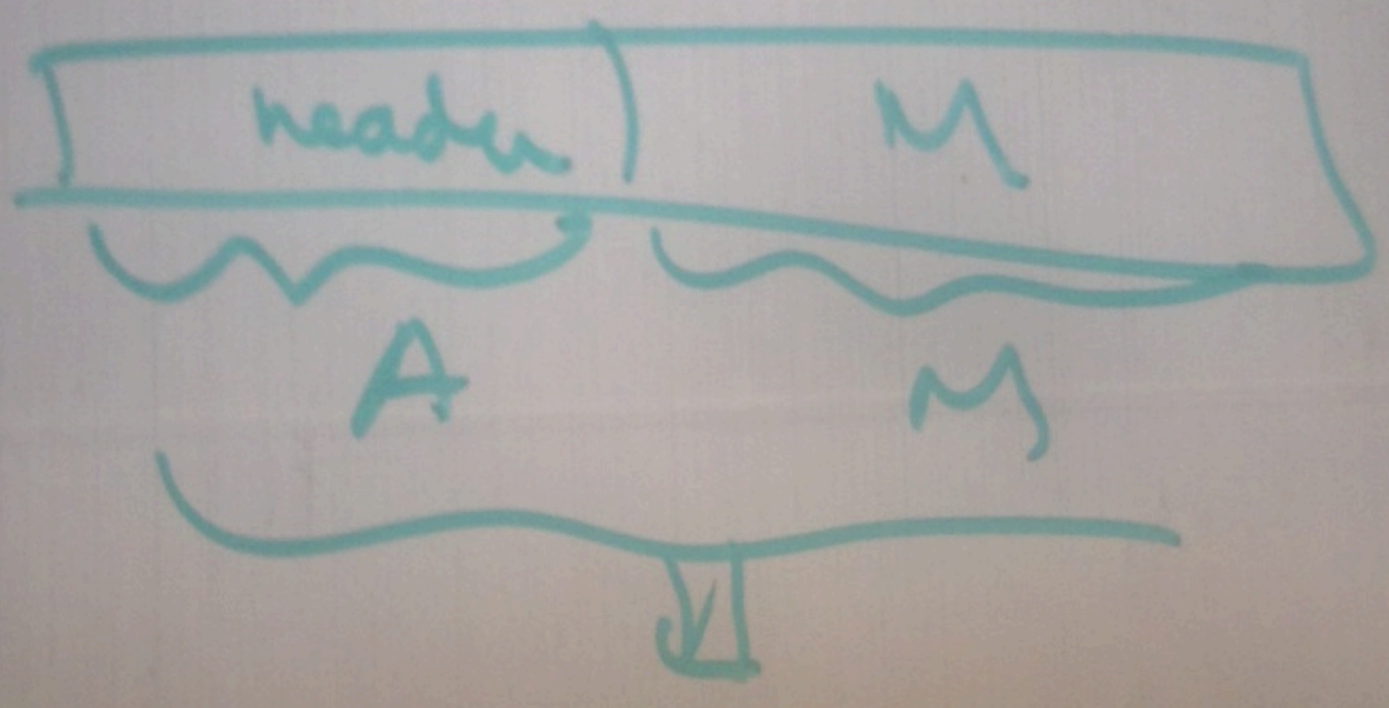
$\overline{Enc}(K, M, A) \Rightarrow C$

C, A

$Dec(K, C, A)$

$\Rightarrow$ Error

$\Rightarrow M \Rightarrow$ (1) M, (2) A } nonce



Enc

// GCM
CCM
OCB