"Eve"

RSA Signature Attack (Multiplicative Attack)

(M_1, S_1) ← Message, Signature → (M_2, S_2) — Known pairs

If $M = (M_1 * M_2) \bmod n \iff S = (S_1 * S_2) \bmod n$

Proof

$$S = (S_1 * S_2) \bmod n$$

$$= (M_1^d \bmod n * M_2^d \bmod n) \bmod n$$

$$= (M_1^d * M_2^d) \bmod n$$

$$= (M_1 * M_2)^d \bmod n$$

$$= M^d \bmod n$$

∴ If Eve knows valid pairs (M_1, S_1), (M_2, S_2) then she can fool Bob by creating $M = M_1 * M_2$, which is multiplicative attack on RSA Signature.

It is also an example of existential forgery.

Note: Signature is over Message only.

☆ Let's say signature is over Message Digest rather than over Message

i.e. (M_1, S_1), (M_2, S_2) } are known

where $S_1 = (h(M_1))^d \bmod n$

$S_2 = (h(M_2))^d \bmod n$

$S_1 * S_2 \bmod n$

$= [(h(M_1))^d * (h(M_2))^d] \bmod n$

$= [h(M_1) * h(M_2)]^d \bmod n$

$= [h(M)]^d \bmod n$

where $h(M) = h(M_1) * h(M_2)$

But existential forgery is relatively hard to implement because knowing $h(M)$, we need to find M

↓

Pre-image is M

↓

But it is ~~Computationally difficult~~