RSA Problem:

mamy 2 liczby pierwsze p, q

$N = p \cdot q$

$\varphi(N) = (p-1)(q-1)$

$e \in \{1 \dots \varphi(N)\}$

dobieramy d:

$ed = 1 \mod \varphi(N)$

(możliwe, bo euklides)

e - klucz publiczny

d - prywatny

$f(x) = x^e \mod N$

mając dane $(f(x), e, N)$ trudno jest znaleźć x

(odwrotność funkcji)

1. Funkcjonalność jak w podpisie Schnorra

1) $P[\quad] = 1$

2) $P[\quad] \leq negl(\lambda)$

Jak wygląda podpis RSA

$(N, e, d) \leftarrow KeyGen(\lambda)$

public: e, N ; private: d

Sign (m, pk, sk)

$e, N \quad d$

$h = H(m)$

ret. $\sigma = h^d \bmod N$

Verify (m, pk, σ):

$h = H(m)$

return $\sigma^e == h$

1. Correctness.

$$L = \sigma^e = (h^d)^e = h^{de} \overset{?}{=} h = P \quad (de \equiv 1)$$

↓ z równości fermata

$$a^{\varphi(N)} \bmod N = a$$

$$a^{k \cdot \varphi(N)} \bmod N = a$$

2. Security

1° Symulacja $O_{sign}()$, $O_{Hash}()$

2° ~~Złamanie~~ ~~problemu~~ Podanie ~~sg~~ messagea do złamania

Zakładamy, że A zrobi ~~q~~ queries do O_{sign} i w j-tej ~~bę~~ zajmie się łamaniem

	m	h	σ
$i \neq j$	m_i	2° r^e	1° r
j		y	$\perp$

(obok wiersza $i \neq j$:) → przejdzie weryfikację $\sigma^e = r^e == h$ OK

(obok wiersza j:) → m on poda σ: my weryfik $\sigma^e \overset{?}{=} y$

→ $\frac{1}{q}$ - pstwo, że odgadniemy dobrze ten moment