Электронная подпись

Свойства подписи:

1. От своей настоящей подписи нельзя отказаться
2. Нельзя подделать
3. В случае конфликта можно проверить подлинность

Будем использовать хэш функцию $h : \{0,1\}^* \to \{0,1\}^s$

$s = 256, 512 \dots$

$h(x) = y$ – необратимая ф-я

Рассмотрим эл. подпись на основе RSA

секр. ключ	откр. ключ
$P_A\ Q_A$	$N_A = P_A \cdot Q_A$
c_A	d_A

$c_A \cdot d_A = 1 \mod (P_A - 1)(Q_A - 1)$

c_A - случ. d - обобщ. алг. Евклида

Алиса передает свое сообщение

$\langle \underbrace{\text{Боб, привет}}_{m}\ y \rangle$

$\widetilde{y =} (h(m_1, \dots, m_k))^{c_A} \mod N_A$

Боб получив проверяет подпись

$h(\tilde{m}_1, \dots, \tilde{m}_k) = \tilde{y} \overset{?}{=} y^{d_A} \mod N_A$

Пример $P_A = 5$ $Q_A = 1$ $m = \{..\}$ $h(m) = 2$

$N_A = 55$ $c_A = 3$ $d_A = 27$ $y = 2^3 = 8$

$\tilde{y} = 8^{27} \mod 55 = 2$ ✓

d_A:

40	1	0	
3	0	1	
1	1	-13	13
0		↑	

+40 = 27