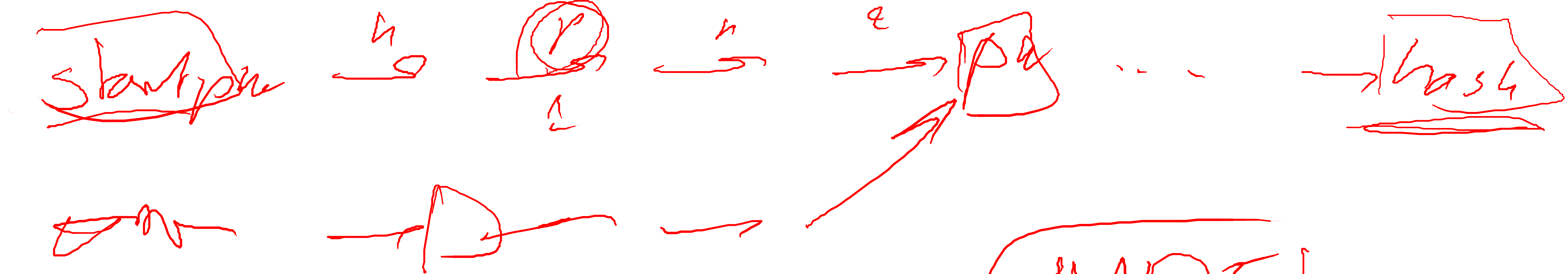


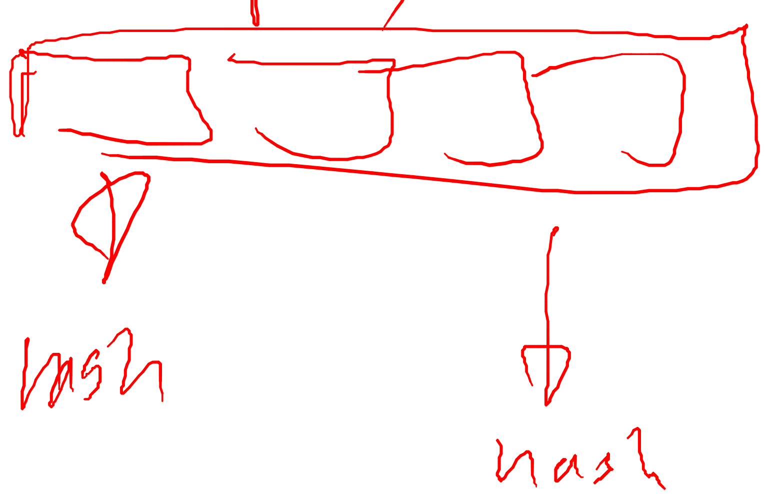
hash ∈ N + i

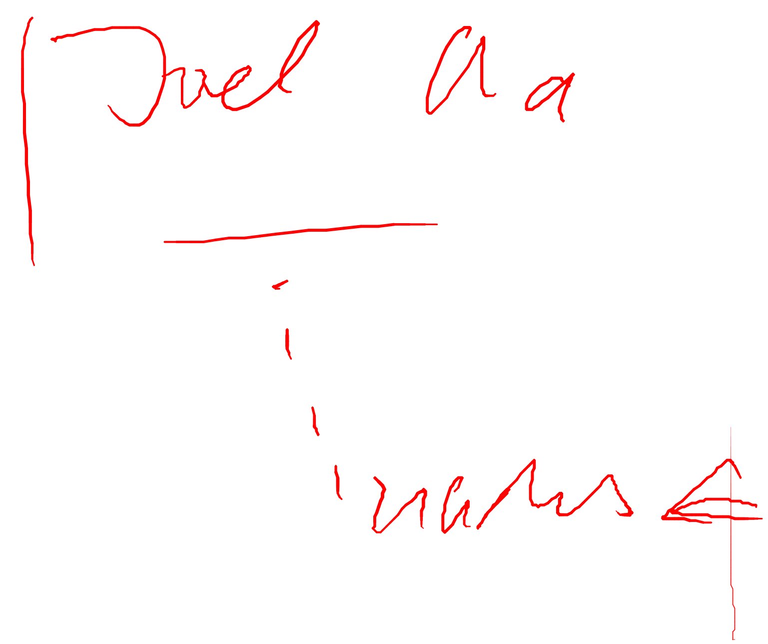
MD5
SHA1
~~CTMC~~

4Bytes

aa = 0
ba = 1
bc 26

Copy-Stop





$$
\begin{array}{r}
4\,7\,8\,1 \\
+\;9\,0\,1\,2 \\
\hline
13'293
\end{array}
\qquad
\begin{array}{r}
\longrightarrow 6 \\
\longrightarrow 3 \\
\hline
0
\end{array}
$$

módulo 9:

$7+4=6$

$6+7=4$

$3\cdot 3=0$

módulo 7

$7\cdot 3=6$

$3\cdot 4=5$

$5\cdot 4=3$

~~$6\cdot x=1$~~

$b^e \bmod n$

$1000 \equiv 10 \pmod{100}$

$\left(10^{1000}\right)^{1000} = 10^{100 \cdot 10^{100}}$.

$= 10^{10^{1003}}$

$= 10$.

$\underbrace{3 \cdot 4 \cdot 5}_{5} \cdot 6 = 3$

$b^e = b^0 \cdot 10^{100} \cdot 10^{1000} =$

$e = 0b1010001 \quad 10^{2000}$

$= 1 + 2 + 32 + 128 = 163$

$b^{163} = \underline{b^{1+2+32+128}} = \underline{b \cdot b^2} \cdot b^{32} \cdot b^{128}$

$b \to b^2 \to b^4 \to (b^4)^2 = b^8$

$(b^2)^2$

$$a^e = x$$

$e = \log_a(x)$ modulo n

symmetrisch

public/private key

AES

Diffie-Hellmann

Alice : p prim

Zufallszahl zahl a (geheim)

Basis b < p

$\longrightarrow p, b, : b^a \bmod p$

Bob Zufallszahl c, $(b^a)^c$

$\longrightarrow$ b^c

Alice : $(b^c)^a$ $b^{a \cdot c}$

RSA:

Modulus $n = p \cdot q$ (p, q prim)

öffentlicher Exp e

privater Exp c

$$\left(x^e\right)^c = x = \left(x^c\right)^e \mod n$$

$$y \longrightarrow \left(y^e\right)^c = y$$

$$\left(h(y)\right)^e$$