

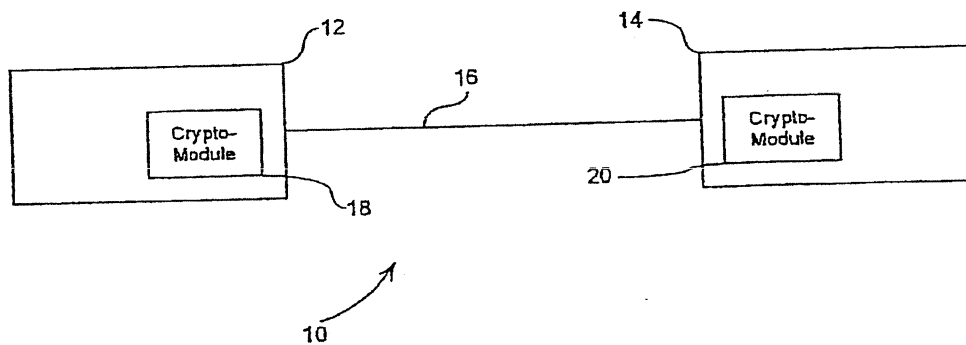


Figure 1

Signer 12

Verifier 14

generate (r, s) and m

derive c

substitute s with c

$(r, c), m$ $\longrightarrow$ $(r, c), m$

compute $e = H(m)$

compute $W = eP + rQ$

$x = \log_W(cR)$

$s = c / x \bmod n$

obtain (r, s) and verify if desired

Figure 2

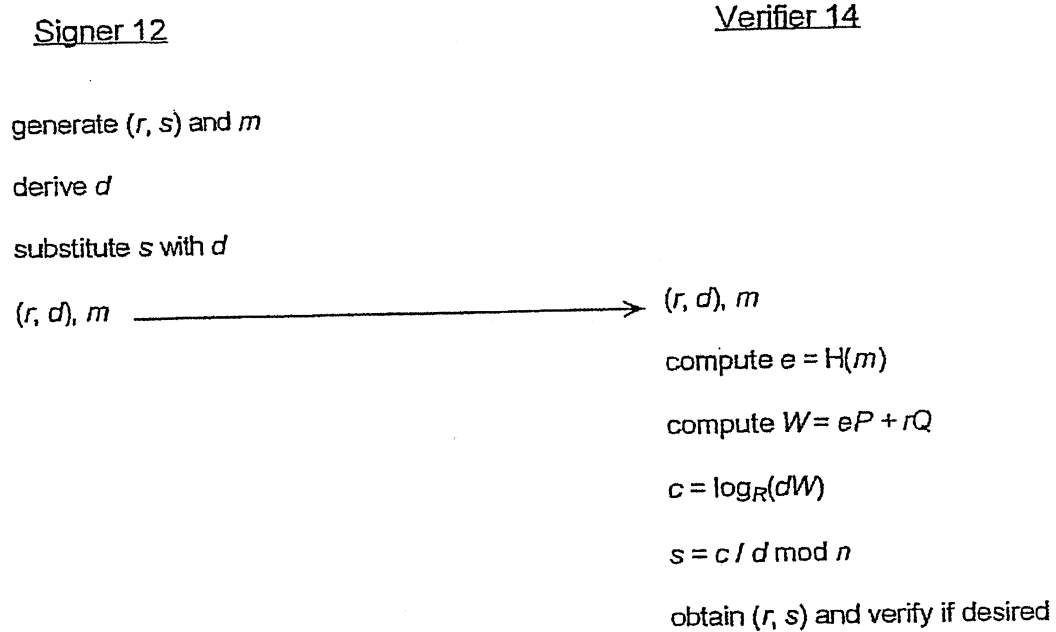


Figure 3