10.4.3 DSA Sign$(x) = (r, s)$

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $r \equiv (\alpha^{k_E} \bmod p) \bmod q$.
3. Compute $s \equiv (SHA(x) + d \cdot r) {k_E}^{-1} \bmod q$.

10.4.4 DSA Vrfy$(x, (r, s))$

1. Compute auxiliary value $w \equiv s^{-1} \bmod q$.
2. Compute auxiliary value $u_1 \equiv w \cdot SHA(x) \bmod q$.
3. Compute auxiliary value $u_2 \equiv w \cdot r \bmod q$.
4. Compute $v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \bmod q$.
5. The verification $ver_{k_{pub}}(x, (r, s))$ follows from:

$$v \begin{cases} \equiv r \bmod q \implies \text{valid signature} \\ \not\equiv r \bmod q \implies \text{invalid signature} \end{cases}$$

Exercise 10.4.6

Set $p = 59$, $q = 29$, $\alpha = 3$, $d = 7$, $\beta = \alpha^d \pmod{59}$. Assuming that $SHA(x) = 26$ compute the DSA signature (r, s).

$p = 59$

$q = 29$

$\alpha = 3$

$d = 7$

$SHA(x) = 26$

$(r, s) = ?$

$\beta = \alpha^d \bmod p = 3^7 \bmod 59 = 3^3 \cdot 3^3 \cdot 3 = 4 \bmod 59$

for this exercise we need to choose an arbitrary k_E, s.t. $0 < k_E < q$

For simplicity, I take $k_E = 1$

At the exam **I suppose** that the professor would choose this value for you, since we're dealing with a MCQ.

$r = \beta \bmod q = (\alpha^{k_E} \bmod p) \bmod q =$

$= (3^1 \bmod 59) \bmod 29 = 3 \bmod 29$

$s = (SHA(x) + d \cdot r) k_E^{-1} \bmod q =$

$= (26 + 7 \cdot 3) \cdot 1^{-1} \bmod 29 = 18 \bmod 29$

My DS is $(3, 18)$, using $k_E = 1$

$K_E = 2$

$r = (3^2 \bmod 59) \bmod 29 = 9$

$s = (26 + 7 \cdot 9) \cdot 2^{-1} \bmod 29 = 2 \cdot 2^{-1} \bmod 29 = 1$

My DS is $(9, 1)$, using $K_E = 2$

$K_E = 3$

$r = (3^3 \bmod 59) \bmod 29 = 27$

$s = (26 + 7 \cdot 27) \cdot 3^{-1} \bmod 29 = \underset{4}{\cancel{12}} \cdot \underset{1}{\cancel{3}}^{-1} \bmod 29 = 4$

My DS is $(27, 4)$, using $K_E = 3$

$K_E = 4$

$r = (3^4 \bmod 59) \bmod 29 = 22$

$s = (26 + 7 \cdot 22) \cdot 4^{-1} \bmod 29 = \underset{3}{\cancel{6}} \cdot \underset{2}{\cancel{4}}^{-1} \bmod 29 =$

$= 3 \cdot 15 \bmod 29 = 16$

*$2^{-1} \bmod 29 \rightarrow 2x \equiv 1 \bmod 29$

EEA $29 = 14 \cdot 2 + 1$

$1 = 29 - 14 \cdot 2 \rightarrow x \equiv -14 \bmod 29 = 15$

My DS is $(22, 16)$, using $K_E = 4$

VERIFICATION

I have (r, s), let's verify the s.s.!

$SHA(x) = 26$

$p = 59$

$q = 29$

$\alpha = 3$

$d = 7$

$\beta = \alpha^d \bmod p = 4 \bmod 59$

- case $(\overset{r}{22}, \overset{s}{16})$

EEA $16x \equiv 1 \bmod 29$

$w = s^{-1} \bmod q = 16^{-1} \bmod 29 = 20 \bmod 29$

$u_1 = w \cdot SHA(x) \bmod q = 20 \cdot 26 \bmod 29 = 27 \bmod 29$

$u_2 = w \cdot r \bmod q = 20 \cdot 22 \bmod 29 = 5 \bmod 29$

$v = (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \bmod q$

$= (3^{27} \cdot 4^5 \bmod 59) \bmod 29 = 22 \bmod 29$

$3^{27} \bmod 59$? $27_{10} = 11011_{bin}$

1. $1^2 \cdot 3^1 = 3 \bmod 59$
1. $3^2 \cdot 3^1 = 27 \bmod 59$
0. $27^2 \cdot 3^0 = 21 \bmod 59$
1. $21^2 \cdot 3^1 = 25 \bmod 59$
1. $25^2 \cdot 3^1 = 46 \bmod 59$

$4^5 \bmod 59$?

$4^2 \cdot 4^2 \cdot 4 = 21 \bmod 59$

$46 \cdot 21 \bmod 59 = 22 \bmod 59$

VERIFICATION CHECK

$$v \begin{cases} \equiv r \bmod q & \checkmark \\ \not\equiv r \bmod q & \times \end{cases}$$

in our case $v \equiv 22 \bmod 29 \equiv r \bmod 29$ O.K.