H(M) = 9, p = 59, q = 29, h = 3, xA = 19, k = 25

a, yA = ?

g = h (p – 1)/q mod p

* g = 3(59-1)/29 mod 59 = 32 mod 59 = 9

yA = gxA mod p = 919 mod 59 = 36

919 mod 59 = [(99 mod 59)2 . 9 ] mod 59 = 36

99 mod 59 = [(94 mod 59)2 . 9] mod 59 = 57

94 mod 59 = 12

Vậy yA = 36

b, (r, s) = ?

r = (gk mod p) mod q

s = [k-1 (H(M) + xr)] mod q

r = (925 mod 59) mod 29

925 mod 59 = [(912 mod 59)2 . 9] mod 59 = 5

912 mod 59 = (96 mod 59)2 mod 59 = 17

96 mod 59 = (93 mod 59)2 mod 59 = 28

93 mod 59 = 21

s = [k-1 (H(M) + xr)] mod q = (25-1 . (9 + 19.5)) mod 29

25-1 mod 29 = 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Q | A1 | A2 | B1 | B2 |
|  | 0 | 29 | 1 | 25 |
| 1 | 1 | 25 | -1 | 4 |
| 6 | -1 | 4 | 7 | 1 |

s = (7 . 104) mod 29 = 3

Vậy (r, s) = (5, 3)

c, w = (s)-1 mod q

u1 = [H(M)w] mod q

u2 = (r)w mod q

v = [(gu1 yu2) mod p] mod q

Kiểm tra: v = r

W = 3-1 mod 29 = 10

U1 = (9.10) mod 29 = 3

U2 = (5.10) mod 29 = 21

V = (93. 3621) mod 59

93 mod 59 = 21

3621 mod 59 = (3610 mod 59)2 . 36] mod 59 = 48

3610 mod 59 = (365 mod 59)2 mod 59 = 27

365 mod 59 = 26

* v = [(21.48) mod 59 ] mod 29 = 5

Vậy v = r => chữ ký đúng (được xác minh)