(1) Initial setup is same as Elgamal encryption

1. Alice chooses a large prime p and primitive root α

2. She then chooses int z & calculates

$\beta \equiv \alpha^z \bmod p$

value of p, α, β are public

z is private

In order to sign the message m Alice follows

1. selects int k such that $GCD(k, p-1) = 1$

2. ~~then~~ computes $r \equiv \alpha^k \pmod p$

3. Finally computes $k^{-1}(m - zr) \pmod{p-1}$

message is triplet (m, r, s)

verification

$v_1 \equiv \beta^r r^s \pmod p$ & $v_2 \equiv \alpha^m \bmod p$

signature is valid if $v_1 \equiv v_2 \bmod p$

(2A) $q = 19$ & $\alpha = 3$ $\alpha = 10$

Alice computes her key

a chooses $x_A = 16$ & $y_A = 10^{16} \bmod 19 = 4$

Alice signs message with $m = 14$ as $(3, 4)$

choosing $k = 5 \Rightarrow gcd(19, 1) = 1$

$s_1 = 10^5 \bmod 19 = 3$

~~s_2~~

$k^{-1} \bmod (q-1) = 5^{-1} \bmod 18 = 11$

$s_2 = 11(14 - 16 \cdot 3) \bmod 18 = 4$

user ~~send~~ B

$v_1 = 10^{14} \bmod 19 = 16$

$v_2 = 4^3 \times 3^4 = 5184 = 16 \bmod 19$

$\Rightarrow 16 = 16$

$v_1 = v_2$

valid

17810165

Sign

3) a) If $y_i = y_j$ for $i \neq j$, then

$$y_{i-1} \oplus x_i = y_{j-1} \oplus x_j$$

As y_{i-1} and y_{j-1} are known, we can deduce the value

$$x_i \oplus x_j = y_{i-1} \oplus y_{j-1}$$

b) using birthday paradox, we know the probability of finding a collision when we have $n = \theta\sqrt{2^{64}}$ blocks at disposal is approximately equal to $1 - e^{-\theta^2 2}$