Homomorphic Encryption

It is a form of encryption that allows users to perform binary operations on encrypted data without ever decrypting the data
[It helps us to outsource information to third party storages for storing and processing without giving access to raw data]

Other encryption:

encrypted data → decrypt data → perform computation → encrypt again

Homomorphic encryption:

encrypted data → perform computation

Types of homomorphic encryption

- Partially homomorphic encryption (PHE)
  - Only one operation but infinite number of times (Only addition or multiplication)
- Somewhat homomorphic encryption (SHE)
  - both addition and multiplication but limited number of times.
- Fully homomorphic encryption (FHE)
  - both addition and multiplication ~~but~~ and infinte number of times.
  - Also perform arbitary computation on data.

Paillier Crypto System

It is a partial homomorphic encryption (PHE) Scheme that works as additively homomorphic in nature

- Only addition, not multiplication

Key generation

1. Choose two prime number p & q randomly and independently of each other such that gcd $(pq, (p-1), (q-1)) = 1$. This property is assured if both primes are of ~~a~~ equal length.
2. Compute $n = pq$ and $\lambda = lcm(p-1, q-1)$
3. Select random integer g where $g \in Z^*{n^2}$
4. Ensure n divides the order of g by checking the ~~existing~~ existence of the following modular multicaptive inverse: $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod$ where fonction L is defined as $L(x) = \frac{x-1}{n}$
   - public (encryption) key is (n, g)
   - private (decryption) key is (λ, μ)

Encryption

1. Let m be message $0 \leq m < n$
2. Select random r where $0 \leq r < n$
3. $c = g^m . r^n \bmod n^2$

Decryption

$m = L(c^\lambda \bmod n^2) . \mu \bmod n$

[Z^* the set where the number set of integers between 1 and n and that are relatively prime to n]

Paillier ecosystem properties:-

- Homomorphic addition of plain text

  The product of two cipher text will decrypt to the sum of their corresponding plain text

  $$D(E(m_1) * E(m_2) \bmod n^{\wedge}2) = (m1 + m2) \bmod n$$

- Homomorphic multiplication of plain text

  A cipher text raised to the power of a plain text will decrypt ~~the~~ to the ~~sum~~ product of two plain text

  $$D(E(m_1)^{m_2} \bmod n^2) = (m_1 * m_2) \bmod n$$