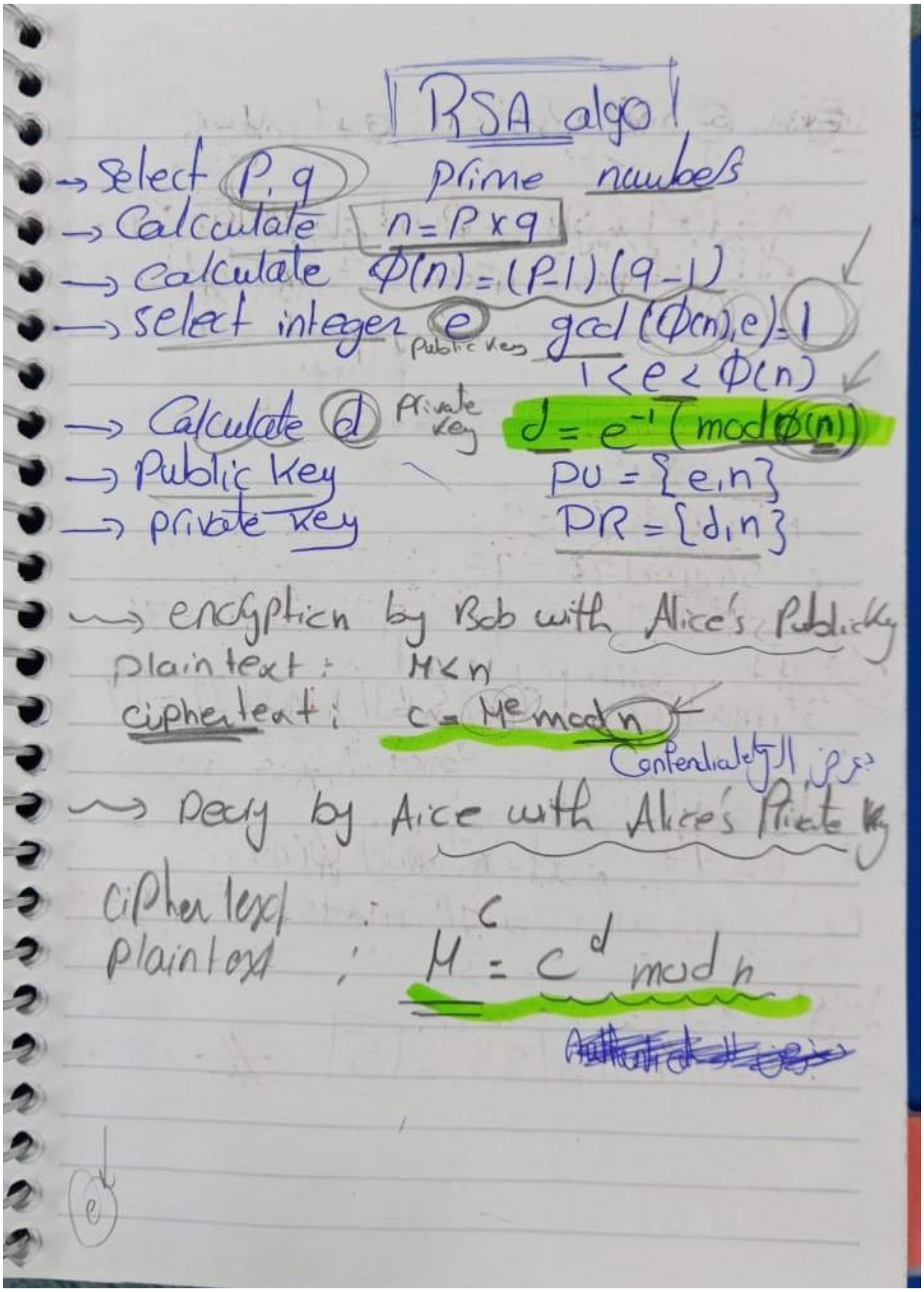
RSA Report

Name: nada osman abdalaziz osman

Sec:2

BN:30



RSA algo

- → Select p, q prime numbers
- → Calculate $\boxed{n = p \times q}$
- → calculate $\phi(n) = (p-1)(q-1)$
- → select integer e Public Key $\gcd(\phi(n), e) = 1$
  $1 < e < \phi(n)$
- → Calculate d Private Key $d = e^{-1}(\bmod \phi(n))$
- → Public Key $PU = \{e, n\}$
- → private key $PR = \{d, n\}$

⤳ encryption by Bob with Alice's Publickey

plaintext : $M < n$

ciphertext ; $c = M^e \bmod n$

يدعم ال Confendialety

⤳ Decy by Aice with Alice's Private key

cipher text : c

plaintext ; $M = c^d \bmod n$

~~يدعم ال Authentication~~

e

Conclusion:

After making encryption and decryption and test them in two way-communication (client and server)

I tried it and it works properly, the server takes the public key of the client then encrypt the message after grouping it to groups consists of 5 characters then it converts and send then the client receives the message group by group and decrypt each one and vice versa and everything saves in a text files (plaintexts, ciphertexts, public-keys)

- After applying the encryption on a different key size, I notice that:

As the key size increases, the time taken for the encryption increases (exponentially from the graph)

And it is logic as it takes more power and calculations but it is more secure then, there is a trade off between security and time, it will be more secure for attacking but it takes much time and power for performing and it is not practical for the systems which needs a real-time

- After applying the attacking on a different key size (used in encryption), I notice that:

As the key size increases, the time taken for the breaking increases

And it is logic as it takes more power and calculations to break the key and know the message, we apply this attack by taking the public-key (e, n) and take the prime factorization of (n) to get (p, q) then find phi-n then get the inverse of (e) which is the private key then decrypt the ciphertext to know the message, so as the key size increases the more difficult to break the key to know the message