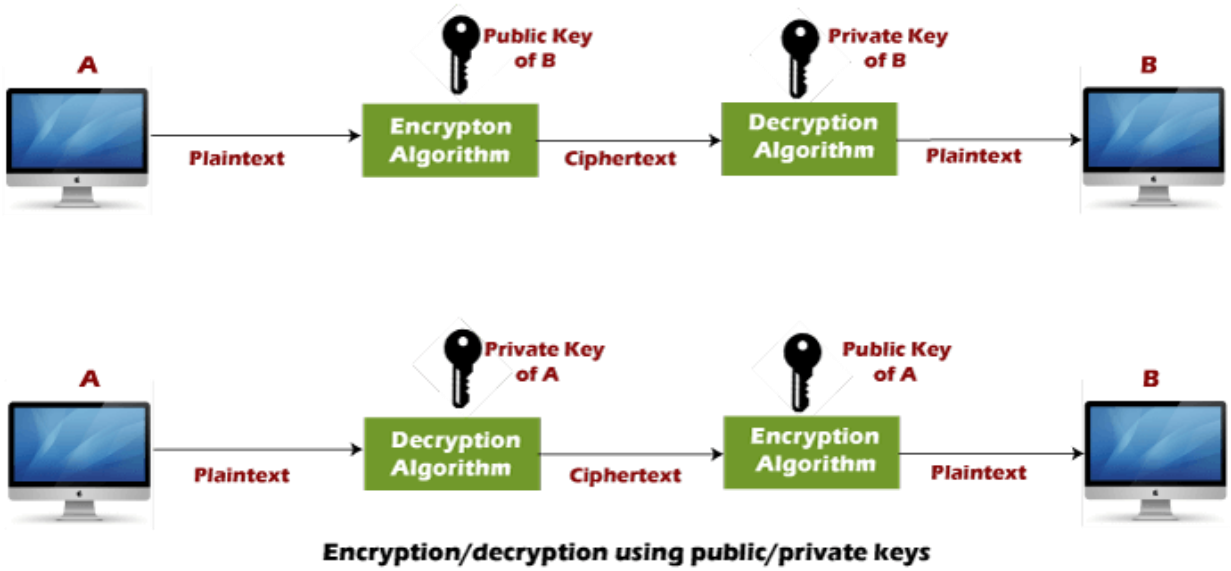
Algoritmi RSA

Algoritmi RSA është një lloj algoritmi me çelës publik ose ndryshe quhen edhe asimetrik. Algoritmet asimetrike janë ato algoritme në të cilat dërguesi dhe pranuesi përdorin çelësa të ndryshëm për enkriptim dhe dekriptim.

Secilit dërgues i caktohen 2 çelësa: çelësi public dhe çelës privat. Çelësi **publik** përdoret për enkriptim, dhe çelësi **privat** për dekriptim. Dekriptimi nuk mund të bëhet duke përdorur një çelës publik. Dy çelësat janë të lidhur, por çelësi privat nuk mund të rrjedh nga çelësi publik. Çelësi publik është i njohur, por çelësi privat është sekret dhe e di vetëm përdoruesi që e ka në pronësi çelësin.

Algoritmi i çelësit publik funksionon në mënyrën e mëposhtme:

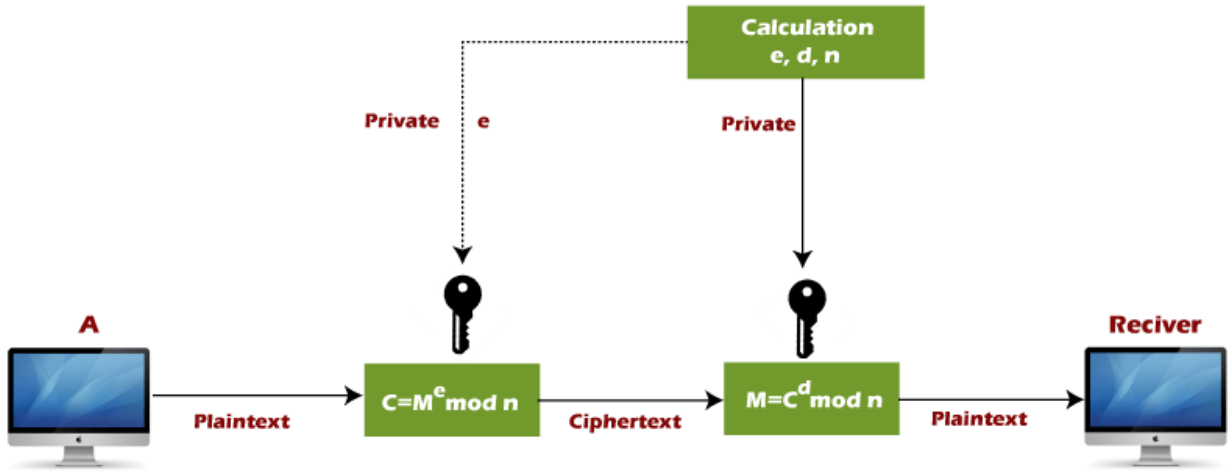
- Të dhënat që do të dërgohen enkriptohen nga dërguesi **A** duke përdorur çelësin publik të pranuesit të synuar B
- B dekripton tekstin e shifruar të marrur duke përdorur çelësin e tij privat, i cili është i njohur vetëm për B. B i përgjigjet A-së duke enkriptuar mesazhin e tij duke përdorur çelësin publik të A-së.
- A deshifron tekstin e shifruar të marrur duke përdorur çelësin e tij privat, i cili është i njohur vetëm për të.



Encryption/decryption using public/private keys

Algoritmi i enkriptimit RSA:

RSA është algoritëm me çelës publik, i quajtur sipas autorëve të tij **Rivest, Shamir dhe Adelman (RSA).**

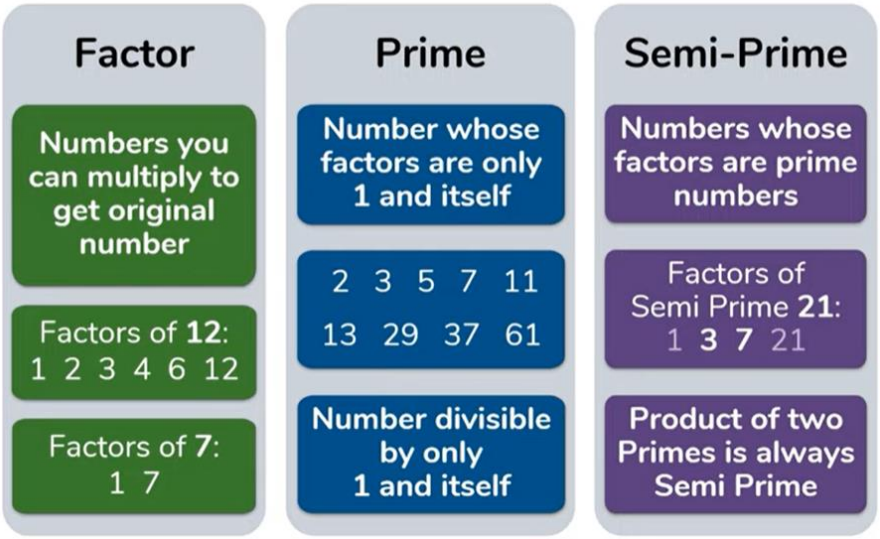


RSA

Algoritmi RSA përdor procedurën e mëposhtme për të gjeneruar çelësa publikë dhe privatë:

- Zgjedhën dy numra të thjeshtë të mëdhenj, **p** dhe **q** .
- Shumëzohen këta numra për të gjetur **n = pxq,** ku **n** quhet moduli për enkriptim dhe dekriptim.
- Zgjedhni një numër **e** më të vogël se **n**, të tillë që n të jetë
    - numër prim(numrat prim janë numra të plotë më të mëdhenj se 1 që kanë vetëm dy faktorë, 1 dhe vetë atë numër),
    - duhet të jetë më i vogël se **(p - 1) x (q -1),**
    - gjithashtu **e** nuk duhet të jetë factor i **(p - 1) x (q - 1)**.
        - **Pra (p-1)x(q-1) Mod e != 0**

Këtu janë disa prej numrave prim deri 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97



- Nëse **n = pxq,** atëherë çelësi publik është <e, n>. Një mesazh me tekst të thjeshtë **m** është i enkriptuar duke përdorur çelësin publik <e, n>. Për të gjetur tekstin e shifruar nga teksti i thjeshtë formula e mëposhtme përdoret për të marrë tekstin e shifruar C.

  $C = m^e \bmod n$

  Këtu, **m** duhet të jetë më e vogël se **n** .

  Për të përcaktuar çelësin privat, përdoret formula e mëposhtme për të llogaritur d të tillë që:

  $D_e \bmod \{(p - 1) \times (q - 1)\} = 1$

  Ose

  $(D * e) \bmod \varphi(n) = 1$

- Çelësi privat është <d, n>. Një mesazh me tekst të shifruar **c** dekriptohet duke përdorur çelësin privat <d, n>. Për të llogaritur tekstin e thjeshtë **m** nga teksti i shifruar c përdoret formula e mëposhtme për të marrë tekstin e thjeshtë m. **$m = c^d \bmod n$**

Sa e sigurt është RSA?

- Siguria qëndron në vështirësinë e faktorizimit të numrave gjysmë të thjeshtë
    - Nëse jepet numri 133, a mund të nxirrni 7 dhe 19?
        - Vërtet?... Vërtetoni, cilët janë faktorët e 1909?
- Në vitin 1991, Laboratori RSA krijoi një Sfidë RSA:
    - Lëshoi 54 Gjysmë-Prime numra të madhësive të ndryshme dhe kërkoi të gjinden faktorët e tyre
        - Konkurrenca përfundoi në vitin 2007 - u identifikuan vetëm 12 faktorë
        - Që nga viti 2020, u identifikuan 11 të tjerë (nuk u dhanë para)
            - Numri më i madh i faktorizuar: 829 bit (shkurt 2020)
        - Në 29 vitet e fundit, numri 1024 bit nuk është faktorizuar kurrë
            - Çelësat RSA 1024 bit u rekomanduan standard që nga viti 2002
            - Çelësat RSA 2048 bit u rekomanduan standard që nga viti 2015

1024 bit Semi-Prime number:

```
135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563
```

Ky është një numër gjysmë prime 1024-bit që RSA publikoi në 1991 ky numër deri më sot nuk është faktorizuar kurrë

Shembulli 1:

Numrin 9 duhet ta enkriptojmë duke përdorur algoritmin e enkriptimit me çelës publik RSA.

Hapi 1: Zgjedhim dy numra të mëdhenj të thjeshtë, **p** dhe **q**.

p = 7

q = 11

Hapi 2: Shumëzojmë këta numra për të gjetur **n = pxq,** ku **n** quhet moduli për enkriptim dhe dekriptim.

Së pari, ne llogarisim

n = pxq

n = 7 x 11

n = 77

Hapi 3: Zgjedhim një numër **e** më të vogël se **n** , të tillë që n të jetë relativisht numër prim me **(p - 1) x (q -1).** Do të thotë që **e** dhe **(p - 1) x (q - 1)** nuk kanë faktor të përbashkët përveç 1. Zgjedhim "e" në mënyrë që 1<e < φ (n), e të jetë i thjeshtë me φ (n), gcd (e, d (n)) =1.

φ (n) = (p - 1) x (q-1)

φ (n) = (7 - 1) x (11 - 1)

φ (n) = 6 x 10

φ (n) = 60

zgjedhim tani e-në e thjeshtë relative të 60 si psh 7. Kështu, çelësi publik është <e, n> = (7, 77)

Hapi 4: Një mesazh me tekst të thjeshtë **m** është i koduar duke përdorur çelësin publik <e, n>. Për të gjetur tekstin e shifruar nga teksti i thjeshtë, përdoret formula e mëposhtme

$C = m^e \bmod n$

$C = 9^{7} \bmod 77$

$C = 37$

Hapi 5: Çelësi privat është <d, n>. Për të përcaktuar çelësin privat, ne përdorim formulën e mëposhtme d të tillë që:

$$\mathbf{D_e \bmod \{(p - 1) \times (q - 1)\} = 1}$$

7d mod 60 = 1, që na jep d = 43

7x43 mod 60 = 1

Çelësi privat është <d, n> = (43, 77)

Hapi 6: Një mesazh i enkriptuar **c** dekriptohet duke përdorur çelësin privat <d, n>. Për të llogaritur tekstin e thjeshtë **m** nga teksti enkriptuar c përdoret formula e mëposhtme:

$$\mathbf{m = c^d \bmod n}$$

$m = 37^{43} \bmod 77$

m = 9

Në këtë shembull, teksti i thjeshtë = 9 dhe teksti i enkriptuar = 37

Detyra 2. Te enkriptohet dhe dekriptohet mesazhi m=7

p = 5, q=11

n=pxq=55

φ (n) = (p-1)(q-1)=4x10=40

e=3

c = $7^3 \pmod{55} =$ **13**

d = 3 x d (mod 40) = 1

d = 27

m = $13^{27} \pmod{55} =$ **7**

Detyra 3.

m = 35

p=23, q=41

n = pxq = 23x41=**943**

φ (n) = (p-1)(q-1)= **880**

e = 7

c = 35^{7}(mod 943) = **545**

3 x d (mod 880) = 1 ->**d=503**

m = 545^{503}(mod 943) = **35**

Detyre: Një person A përdor dy numra të thjeshtë, 13 dhe 17, për të gjeneruar çelësat publikë dhe privatë. Nëse celësi publik i A është 35. Atëherë sa është çelësi privat i A ?

p = 13

q = 17

n = pxq

n = 13 x 17 = **221**

llogarisim

φ (n) = (p - 1) x (q-1)

φ (n) = (13 - 1) x (17 - 1)

φ (n) = 12 x 16

φ (n) = 192

Për të përcaktuar çelësin privat, ne përdorim formulën e mëposhtme për të llogaritur d

$d = d_e \bmod \varphi(n) = 1$

d = d x 35 mod 192 = 1

$d = (1 + k \times \varphi(n))/e$ [k =0, 1, 2, 3.....]

Vendos k = 0

d = (1 + 0 x 192)/35

d = 1/35

Vendos k = 1

d = (1 + 1 x 192)/35

d = 193/35

Vendos k = 2

d = (1 + 2 x 192)/35

d = 385/35

d = 11

Çelësi privat është <d, n> = (11, 221)

Prandaj, çelësi privat dmth d = 11

Një kriptosistem RSA përdor dy numra të thjeshtë 3 dhe 13 për të gjeneruar çelësin publik= 3 dhe çelësin privat = 7. Cila është vlera e tekstit të shifruar për një tekst të thjeshtë?

Shpjegim:

Hapi 1: Në hapin e parë, zgjidhni dy numra të thjeshtë të mëdhenj, **p** dhe **q** .

p = 3

q = 13

Hapi 2: Shumëzoni këta numra për të gjetur **n = pxq,** ku **n** quhet moduli për enkriptim dhe deshifrim.

Së pari, ne llogarisim

n = pxq

n = 3 x 13

n = 39

Hapi 3: Nëse **n = pxq,** atëherë çelësi publik është <e, n>. Një mesazh me tekst të thjeshtë **m** është i koduar duke përdorur çelësin publik <e, n>. Kështu, çelësi publik është <e, n> = (3, 39).

Për të gjetur tekstin e shifruar nga teksti i thjeshtë, përdoret formula e mëposhtme për të marrë tekstin e shifruar C.

$C = m^e \bmod n$

$C = 5^3 \bmod 39$

C = 125 mod 39

C = 8

Prandaj, teksti shifror i krijuar nga teksti i thjeshtë, C = 8.

Shembulli 4:

Një kriptosistem RSA përdor dy numra të thjeshtë, 3 dhe 11, për të gjeneruar çelësin privat = 7. Cila është vlera e tekstit të koduar për një tekst të thjeshtë 5 duke përdorur algoritmin e enkriptimit me çelës publik RSA?

Shpjegim:

Hapi 1: në hapin e parë, zgjidhni dy numra të thjeshtë të mëdhenj, **p** dhe **q** .

p = 3

q = 11

Hapi 2: Shumëzoni këta numra për të gjetur **n = pxq,** ku **n** quhet moduli për enkriptim dhe deshifrim.

Së pari, ne llogarisim

n = pxq

n = 3 x 11

n = 33

Hapi 3:

Llogarisim

φ (n) = (p - 1) x (q-1)

φ (n) = (3 - 1) x (11 - 1)

φ (n) = 2 x 10

φ (n) = 20

Hapi 4: Për të përcaktuar çelësin publik, ne përdorim formulën e mëposhtme për të llogaritur d në mënyrë që:

Llogarit exd = 1 mod φ (n)

e x 7 = 1 mod 20

e x 7 = 1 mod 20

e = (1 + k x φ (n))/ d [le k =0, 1, 2, 3.....]

Vendos k = 0

e = (1 + 0 x 20) / 7

e = 1/7

Vendos k = 1

e = (1 + 1 x 20) / 7

e = 21/7

e = 3

Çelësi publik është <e, n> = (3, 33)

Prandaj, çelësi publik dmth e = 3