RSA

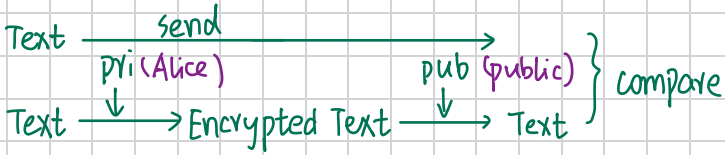
Asymmetric

Can only encrypt short texts (≤ 256 bits)

Data Encryption : Plain Text —pub (Alice)→ Encrypted Text —Pri (Bob)→ Plain Text

Encrypt with public key and decrypt with private key.

Digital Signature:



Encrypt with private key and decrypt with public key.

Select prime numbers p and q let $n = pq$

Euler function $\phi(n) = (p-1)(q-1)$

Select an integer e s.t. $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$

Expand Euclidean: Calculate d as the modular inverse element of e (i.e. $ed \equiv 1 \bmod \varphi(n)$)

Public key (n, e), Private key (n, d)

Encryption:

1. Change Type

Plain text M ⟶ Integer m (s.t. $0<m<n$)

2. Calculate ↓

c s.t. $c \equiv m^e \pmod n$

use only public key

Encrypted Text: C

Decryption:

1. Calculate

Encrypted Text C ⟶ $c^d \equiv m^{de} \equiv m^{k\varphi(n)+1} \equiv m \pmod n$

↓ 2. Change Type

Plain text M

Plain Text: M

Range:

$e = 65537 = 2^{16}+1$ (static)

n has the length of 1024 / 2048 / 4096 (binary)

number of digits depends on n's length (binary)

max plaintext length < n's length

(M ≤ 1024 / 2048 / 4096 bits = 128 / 256 / 512 bytes)

key Cracking:

n ⟶ $n = pq$ time complexity T: $O(n^{\frac{1}{4}}\log n) \le T \le O(\sqrt{n})$

n 1024 bits: $n^{\frac{1}{4}}\log n \approx 2^{256} \cdot 1024 = 2^{256+10}$ times

? PC 3GHz 3 billion times / second

$$\text{Time Cost} = \frac{2^{256+10}}{3\times 10^9} \times \frac{1}{86400\times 365}$$

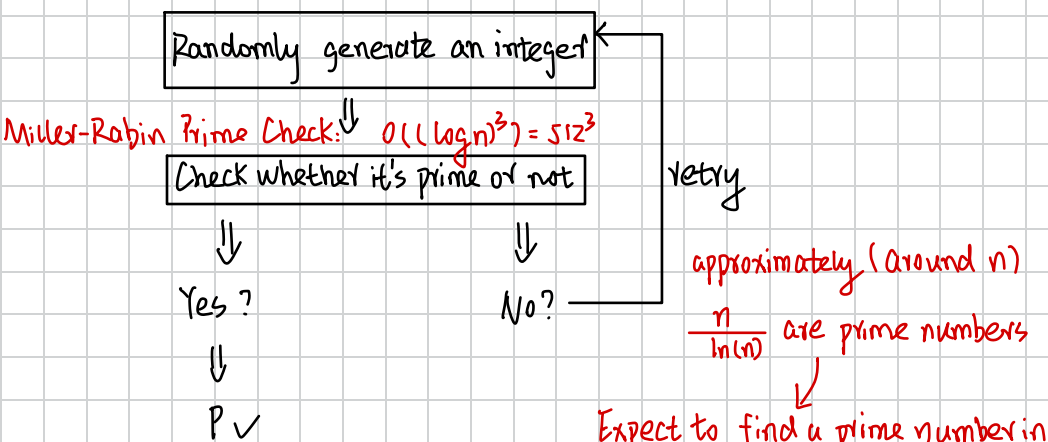
$$\geq 2^{208} \text{ years}$$

? Fugaku 10^{17} times / second

Time cost $\geq 2^{182}$ years

Encryption:

1 Select 512 bits prime number p:



As a result we need $512^3 \times 256 \times e \approx 2^{36}$ times (very slow)

2. Find d s.t. $ed \equiv 1 \pmod{\varphi(n)}$

$O(\log(\min\{e, n\}))$ to Find $ex + \varphi(n)y = 1$

let $d = x$ we have $ed \equiv 1 \pmod{\varphi(n)}$

(Nearly no time cost)

Public key: rsa.pub: 408 bytes

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDY4+zSrbw8KvIEhbXHgxY9S4+/
zyiLCOvAFwENbo9gFhdkcEABa1yemGv+vd8sJPYBaRUAX+l7Z0erxZrC5DvvMnLVLZgGnclGUfPHtpq/
xxK16geFZEW3eHNZA0KN5JyB+naF/Zilc24RHJqiFYHyJtRW884MRmm5/
FXTH3Etj5mZHN4Lhq7xB0JFFjPMwVFQmAHMmHE+kmxSC+Cr5Zkwpidbl0HQDI1Aj6bQRMaUfWmK+ae/
bRe1jBk+1c81ymJSpl4L4gpc1mVYrzjzrEA4WyG/
Z7RMDkMNVLuA1pJIvcFd3IYW8GIlOi5ssnFCTko5pvZEKEUqh6JQj3QgWRQ3 xiezeyu@MyMacBookAir.local
```

Private key: rsa 1831 bytes

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA2OPs0q28PCryBIW1x4MWPUuPv88oiwjrwBcBDW6PYBYXZHBAAWtc
nphr/r3fLCT2AWkVAF/pe2dHq8WawuQ77zJy1S2YBp3JRlHzx7aav8cSteoHhWRFt3hzWQ
NCjeScgfp2hf2YpXNuERyaohWB8ibUVvPODEZpufxV0x9xLY+ZmRzeC4au8QdCRRYzzMFR
UJgBzJhxPpJsUgvgq+WZMKYnW5dB0AyNQI+m0ETGlH1pivmnv20XtYwZPtXPNcpiUqZeC+
IKXNZlWK8486xAOFshv2e0TA5DDVS7gNaSSL3BXdyGFvBiJToubLJxQk5KOab2RChFKoei
UI90IFkUNwAAA9AlZBS4JWQUuAAAAAdzc2gtcnNhAAABAQDY4+zSrbw8KvIEhbXHgxY9S4
+/zyiLCOvAFwENbo9gFhdkcEABa1yemGv+vd8sJPYBaRUAX+l7Z0erxZrC5DvvMnLVLZgG
nclGUfPHtpq/xxK16geFZEW3eHNZA0KN5JyB+naF/Zilc24RHJqiFYHyJtRW884MRmm5/F
XTH3Etj5mZHN4Lhq7xB0JFFjPMwVFQmAHMmHE+kmxSC+Cr5Zkwpidbl0HQDI1Aj6bQRMaU
fWmK+ae/bRe1jBk+1c81ymJSpl4L4gpc1mVYrzjzrEA4WyG/Z7RMDkMNVLuA1pJIvcFd3I
YW8GIlOi5ssnFCTko5pvZEKEUqh6JQj3QgWRQ3AAAAAwEAAQAAAQEAlEuzf5F+5PzQIbty
wQmmSR7DGPkB1Z6x4tNXyuFPcvln4SrG+LF50I6TOMiGMV7MPcalr23k7JV/cblYyezX9g
LedVgJXGzCVCxwrJr0UDBDYNK1dcVLzdiztab++JnZUR35sD/nASldlqGiMTTXdsSJ5zIo
LkhuvdYEsKgM8IK+tBzwGjH7ghNHGkai3dC+b0ehGXGcP8akgQq8hzWWZgITyzsBC5uuaH
Kw1nqsYnznxc9LgHHsiPz9kLvEZj3UbZqSagBreO5/+sZl+P1XgsWQwZRuwKkyF2YkCqeL
LZPjNytUP/JDK4ol8z7ne42iGbCNFl2OMavMfqscj73QMQAAAIBvh8yQBCTc33F7fLbT1X
8SyMhsz43/k43Qv+J5lD41j4eZ9X/RocPkak0uxK16xVnVJCtM6G006Axv4Z7LkBAq3SlE
x6nxcLPDQ+rcqeDcSX1BCufP1ws+yW47vHJLx0QO8QyOiXj+TpcYEjQu350atGAZ+zoONE
OIhejfJK/ODQAAAIEA80jHYFh7vfMlaSR5SjQ/M7kzjPIWK2Q/7UWRlXECkX/iNOhIWSwA
ddhoUeL+MPXKCbxIz4TQ5Ef1sTQOkb+mGYgQJq1ceDLPocPASJX/KFu9EntDkIPkjNh4AR
s2sXkVv4//wCDbCimw0zZf5fcl5rQaIN6qUtwcnKqTVRiPLSMAAACBAOQ5/JhoLdC2f9cn
Ouesb/4UCdt8xAgHtnYASl058BSvJtFLyuEnPJVX/bAfZ4sokjP5HAk8lCbAXD6riOeYSv
UlCnbq384kn0AePNlEGOIoqbGrSdrsX06Rr5ZMMUxP6zABQ9Pwfj1WlT4FrU7qduMzLR0F
XHcO6YqcPZ6bxr/dAAAAGnhpZXpleXVATXlNYWNCb29rQWlyLmxvY2Fs
-----END OPENSSH PRIVATE KEY-----
```