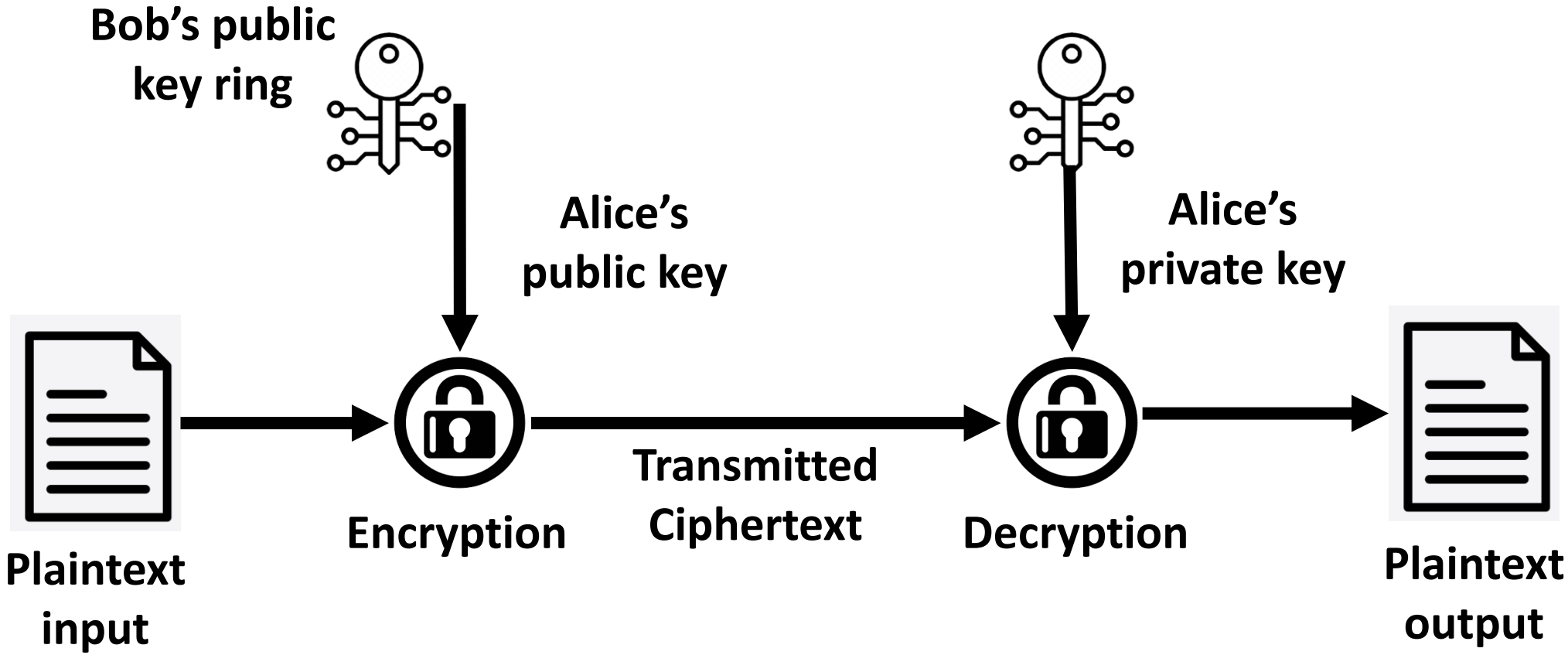
Public key cryptography

Md. Hedayetul Islam

ID: 17702013

Motivation

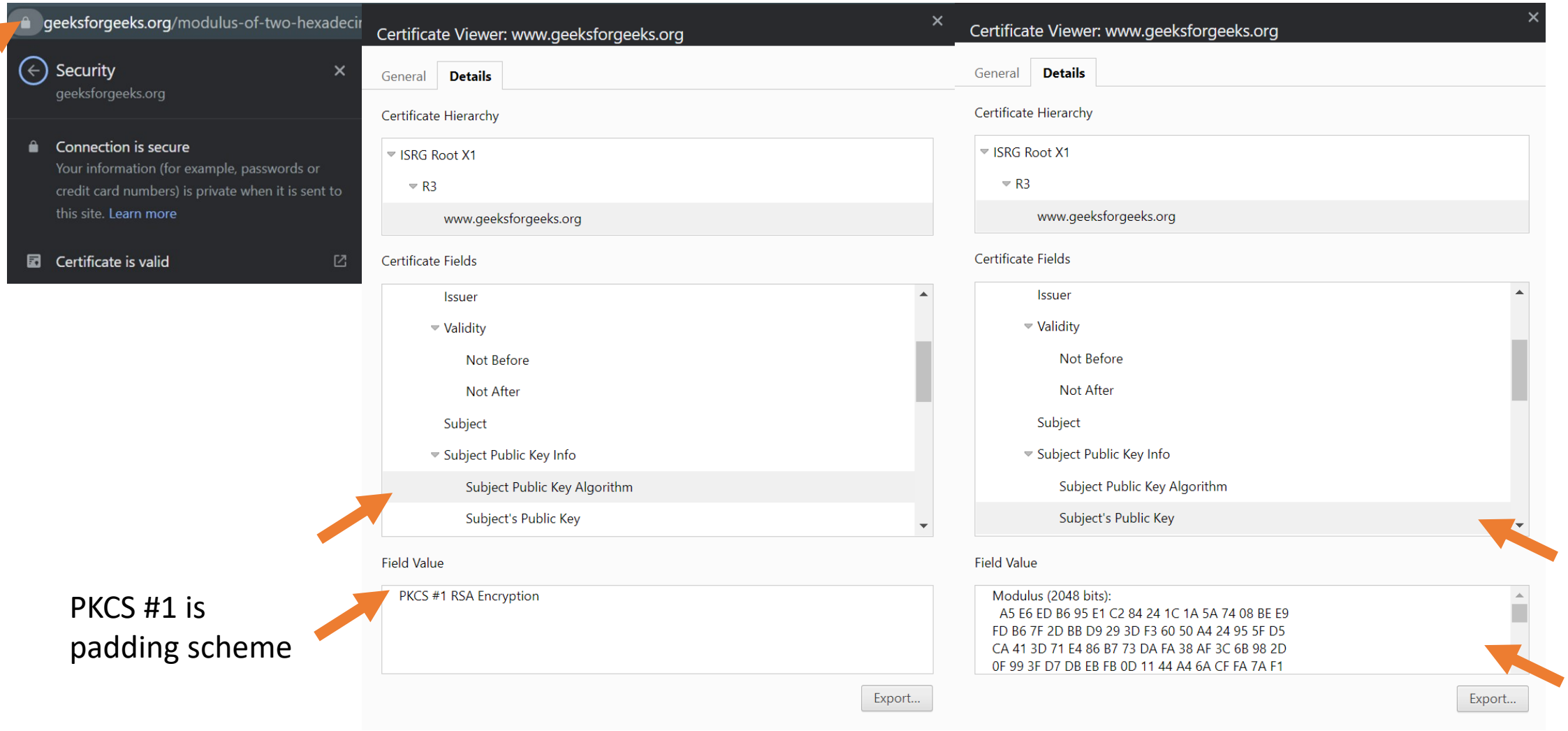


** One key for encryption, Another for decryption

Public key algorithms

- RSA (Rivest-Shamir-Adleman)
- ECDSA (Elliptic Curve Digital Signature Algorithm)
  - Fewer bits than RSA
- DSA (Digital Signature Algorithm)
- Diffie-hellman key agreement protocol

How to check?



PKCS #1 is padding scheme

Modulus length!

```
rsa=b'J5 E6 ED B6 95 E1 C2 84 24 1C 1A 5A 74 08 BE E9 FD B6 7F 2D BB D9 29 3D F3 60 50 A4 24 95 5F D5 CA 41 3D 71 E4 86 B7 73 DA FA 38 AF
3C 6B 98 2D 0F 99 3F D7 DB EB FB 0D 11 44 A4 6A CF FA 7A F1 E7 54 11 68 7A 5D 99 E1 DB B8 65 9E 54 AC 0C 88 74 BC 35 A5 52 90 14 0F 8A BF
A8 ED 31 60 A1 9F B7 81 9F 78 B7 16 F6 AB CD A4 6E E9 53 4D 0C A3 52 B8 18 8D 55 B8 95 FB 69 0D 1F 4A 1A DB F4 D0 F6 17 98 EC 6D 9F A2 FE
BA FD 8A 37 CB 64 B2 A7 AC AD 59 3B CA 32 41 EC 2F 3D 29 E5 E8 2D AF 34 4F 42 83 72 C8 02 95 B5 AD 99 44 77 71 26 D0 E8 EA 27 0D 52 2C 34
CF 3E 0F 57 B1 CF 86 2B 7C 93 D6 B6 73 A8 31 D7 B2 C1 D8 2F 6F 5F 9D 16 40 43 DA 7F 5A 46 74 BB 69 56 22 53 B0 C9 A1 5E E8 73 E6 23 AF A4
01 3D 42 84 9D 14 A5 EF A7 E4 8F 26 83 FB C3 C1 9E 13 C0 54 84 25 3A 7F 5A 2F 73 BB'
```

```
Hence the exponent number is: 3.82E+1846
```

```
ec = b'Z0 04 D8 92 B8 4E 10 09 F6 0F AA 39 E7 A9 23 6E 0F 41 D1 25 76 32 1F D6 F1 13 CE 55 E2 21 1A 8A 39 69 C7 5F 91 3C 88 CA 2F D2 D3
7E F9 80 72 F9 25 3B 41 6B D2 F3 14 93 99 89 30 87 91 3F AA 1F 4D 1B'
```

```
Hence the exponent number is: 9.34E+473
```

Python for check

```
int.from_bytes(rsa, byteorder='big',signed=False)
```

RSA Operation

Key exchange

- *Assume two prime number p and q*
- *Modulus,* $n = p \,.\, q$
- *Eulers tocient function,* $\phi(n) = (p\text{-}1) \,.\, (q\text{-}1)$
- *Choose coprime integer,* $e = \begin{cases} 1 < e < \phi(n) \\ gcd(\phi(n), 1) = 1 \end{cases}$
- $d \equiv e^{-1} \, mod \, \phi(n)$ *hence,* $d.e \equiv mod \, \phi(n)$
- *public key,* $\{e, n\}$
- *private key* $\{d, n\}$

Encryption (Public)

- $Ciphertext, C = M^e mod(n)$

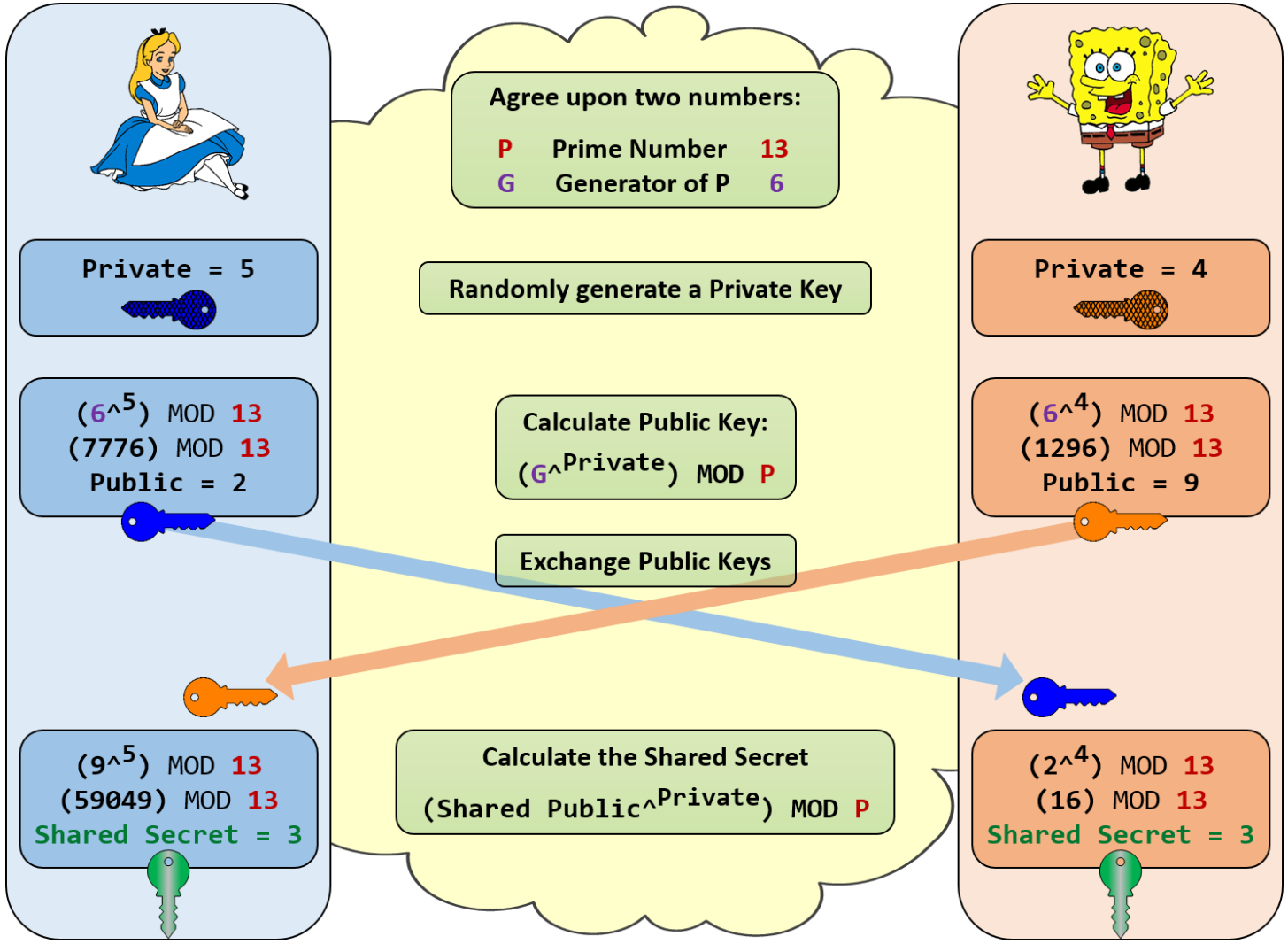
Decryption (Private)

- $Plaintext, M = C^d mod(n)$

For 14 Euler's tocient function is 6,

14 = 1,2,3,4,5,6,7,8,9,10,11,12,13,14

Diffie-Hellman Key exchange



Possible attack on RSA

- Brute-force Attack
- Timing Attack
  - If Eve knows the Alice’s hardware in sufficient details, it is able to measure the decryption time for several known cipher text.
- Chosen cipher attack

Thank you!