# **2550 Intro to** cybersecurity Public key Crypto

abhi shelat

## Recap 1) Perfect Security, ore-time pad ( Symmetrie encoyption, computational security · AES (heuriste) > Short Keyr encrypt · Blum-Micali PPG arbitrary lung messager

3 Asymmetriz cryptography, and public Key cryptography • PSA

#### Revisit our model for Encryption

#### Symmetric key enc has 1 major drawback.

Bob Kas, Kbc Kbd Kbe Kbf Kby

Garol

6150

- each pair nearly for manage a

Dave

~ ...

 $O(n^2)$ 

Keys.

secret key.

Evan

- - -

Francis

Alice Kab, Koc, Kad, Kae, Kaf, Kag

George

#### Symmetric key enc has 1 major drawback.

 $k_{ba}, k_{bc}, k_{bd}, k_{be}, k_{bf}, k_{bg}$ 

 $k_{ca}, k_{cb}, k_{cd}, k_{ce}, k_{cf}, k_{cg}$ Garol

 $k_{da}, k_{db}, k_{dc}, k_{de}, k_{df}, k_{dg}$ Dave

Alice

O(n<sup>2</sup>) keys to manage!

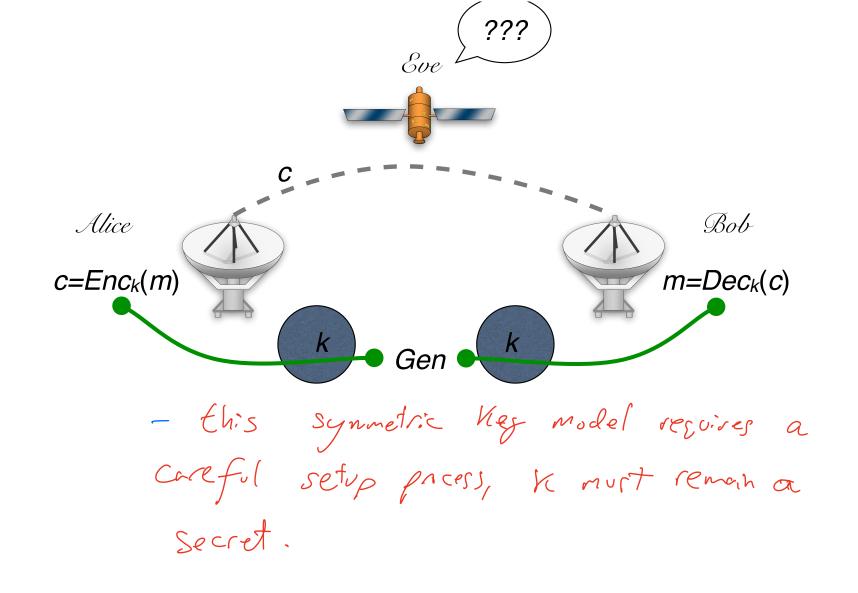
 $k_{ab}, k_{ac}, k_{ad}, k_{ae}, k_{af}, k_{ag}$ 

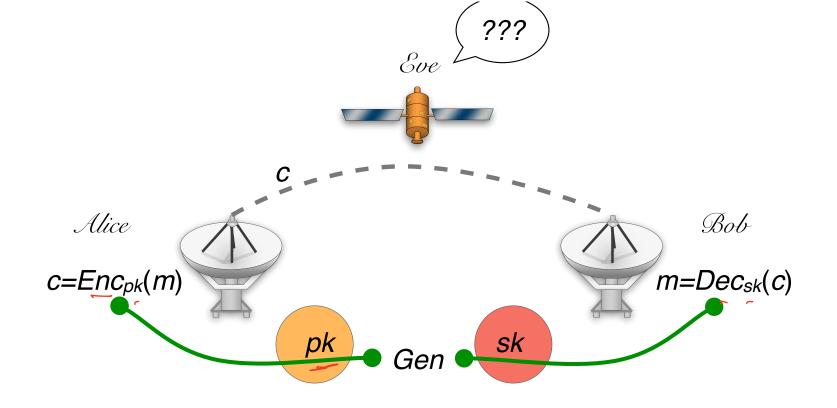
George  $k_{ga}, k_{gb}, k_{gc}, k_{gd}, k_{ge}, k_{gf}$ 

. Evan  $k_{ea}, k_{eb}, k_{ec}, k_{ed}, k_{ef}, k_{eg}$ 

Francis

 $k_{fa}, k_{fb}, k_{fc}, k_{fd}, k_{fe}, k_{fg}$ 





Pk can be used to encrypt.

sk can be used to decrypt.

Asymmetric cryptography

#### PKC key enc

Bob

 $sk_b$ 

 $sk_c$ : Garol

sk<sub>d</sub> Dave

Alice

 $sk_a$ 

*pk<sub>a</sub>*, *pk<sub>b</sub>*, *pk<sub>c</sub>*, *pk<sub>d</sub>*, *pk<sub>e</sub>*, *pk<sub>f</sub>*, *pk<sub>g</sub>* Are publicly posted

Evan sk<sub>e</sub>

George sk<sub>g</sub>

Francis

 $sk_f$ 



Gen Enc Dec 3 algorithms

Gen(key generation)Security<br/>prometer $(pk, sk) \leftarrow Gen(1^n)$ prometerEnc(encryption) $c \leftarrow Enc_{pk}(m)$  for  $pk \in \mathcal{K}, m \in \mathcal{M}$ Dec(decryption)

## Public key encryption

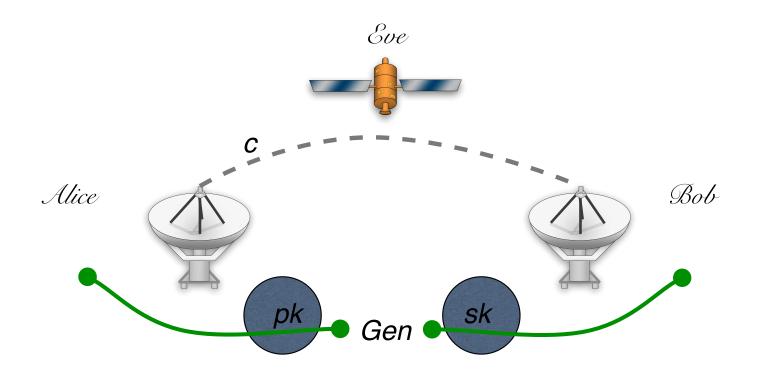
GenEncDec3 algorithms

Gen (key generation)  $(pk, sk) \leftarrow \text{Gen}(1^n)$ 

Enc (encryption)

 $c \leftarrow \mathsf{Enc}_{pk}(m) \text{ for } pk \in \mathcal{K}, m \in \mathcal{M}$ Dec (decryption)

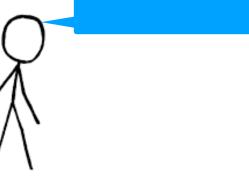
 $\forall m \in \mathcal{M}, (pk, sk) \leftarrow \mathsf{Gen}(1^n)$  $\Pr[\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$ 



"for any pair of messages  $m_1, m_2$ , *Sve* cannot tell whether  $C = EnC_{pk}(m_i)$ ."

(weakest notion of security)

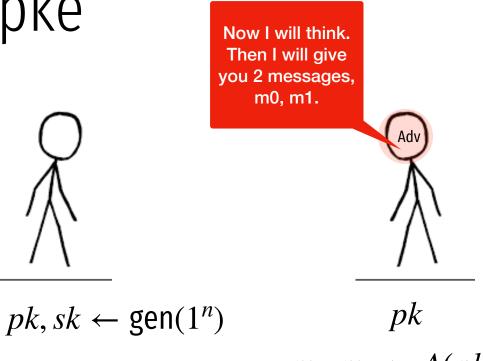
I will make a key pair and give you the public part.



$$pk, sk \leftarrow gen(1^n)$$

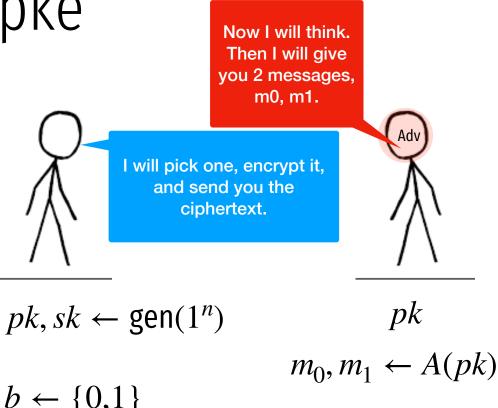
pk

(weakest notion of security)

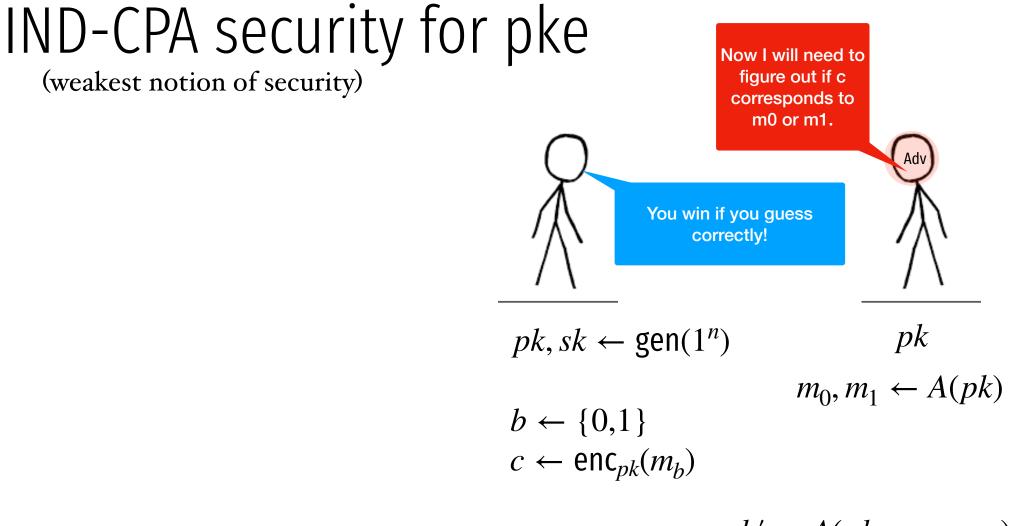


 $m_0, m_1 \leftarrow A(pk)$ 

(weakest notion of security)



$$b \leftarrow \{0,1\}$$
$$c \leftarrow \operatorname{enc}_{pk}(m_b)$$



 $b' \leftarrow A(pk, m_0, m_1, c)$ 

(weakest notion of security)

$$pk, sk \leftarrow gen(1^n)$$
$$m_0, m_1 \leftarrow A(pk)$$
$$b \leftarrow \{0,1\}$$
$$c \leftarrow enc_{pk}(m_b)$$
$$b' \leftarrow A(pk, m_0, m_1, c)$$

$$\Pr[b = b'] \leq 1/2 + \epsilon(n)$$

#### How to build public key encryption?

Lets look a the first such example,

RSA. (D'fextbook versin (insecure)

(2) RSA- OAEP

Basic Number theory

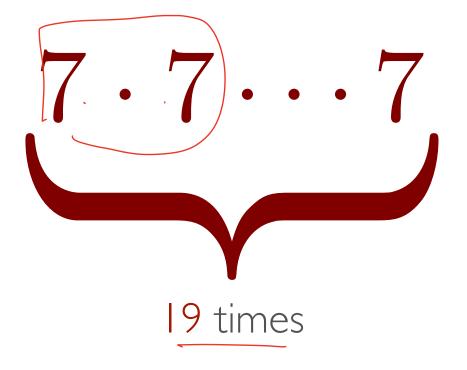
O Modula Exponentiation (9,×10) (Exfinded) (2) Greatest Comon Divisor (GCO) 3 Euler Totient function

=) PSA scheme (1978)

#### Modular Exponentiation

 $(a, x, n) \to a^x \mod n$ 





#### Modular Exponentiation $(a, x, n) \to a^x \mod n$ $7^{19} \mod 31$ food 31) 9 16 7 $7^{16}$ 78 7. 7 14-14= 196 18-18=324 (0-0) = (00)18 7 14 7 1) $7'^{9} = 7'^{6}, 7^{2}, 7'$ $7 \cdot 18 \cdot 7 = 1141$

#### Modular Exponentiation $(a, x, n) \rightarrow a^x \mod n$

 $7^{19} \mod 31$ 

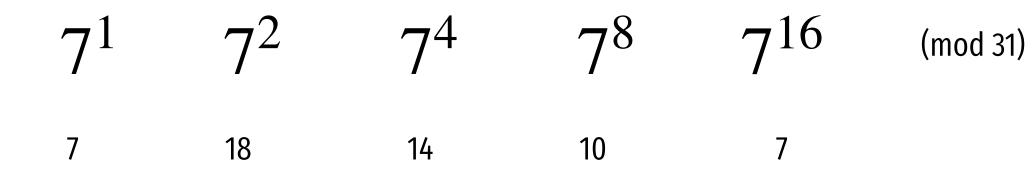
#### Modular Exponentiation $(a, x, n) \rightarrow a^x \mod n$

 $7^{19} \mod 31$ 

 $7^1$   $7^2$   $7^4$   $7^8$   $7^{16}$ (mod 31)

#### Modular Exponentiation $(a, x, n) \rightarrow a^x \mod n$

 $7^{19} \mod 31$ 



#### Modular Exponentiation

 $(a, x, n) \to a^x \mod n$ 

**Algorithm 2**: ModularExponentiation(a, x, n)Input:  $a, x \in [1, n]$ 1  $r \leftarrow 1$ 2 while x > 0 do if x is odd then 3  $| \quad | \quad r \leftarrow r \cdot a \bmod n$ 4  $\begin{array}{c|c} \mathbf{5} & x \leftarrow \lfloor x/2 \rfloor \\ \mathbf{6} & a \leftarrow a^2 \bmod n \end{array}$ 7 Return *r* 

#### Modular Exponentiation

$$(a, x, n) \to a^x \mod n$$
  
 $a^x \mod n = \prod_{i=0}^{\ell} x_i a^{2^i} \mod n$ 

**Algorithm 2**: ModularExponentiation(a, x, n)

Input:  $a, x \in [1, n]$  $r \leftarrow 1$ 2 while x > 0 do | if x is odd then $| r \leftarrow r \cdot a \mod n$  $| x \leftarrow \lfloor x/2 \rfloor$  $| a \leftarrow a^2 \mod n$ 7 Return r

#### Greatest Common Divisor $A^{7\beta}$ $GCD(A,B) = GCD(B, A \mod B)$

 $GCD(A,B) = GCD(B, A \mod B)$ 

 $GCD(6809, 1641) \leq$ 

- =GCO(1641, 245)
- = GCD( 245, 1641 mod 275=171)
- = GCD(171, 74)

6809 = 4.1641 + 2451641 = 6.245 + 171245 = 1.(71 + 74)

GCD(6809,1641) GCD(1641, 245) GCD(245, 171) GCD(171, 74) GCD(74, 23) GCD(23, 5) GCD(5, 3)GCD(3, 2)GCD(2, 1)

6809 = 4.1641 + 2451641 = 6-245 + 171 245 = 1.171 + 74171=2.74 + 23 77=3.23+5 23 = 4.5 + 3  $5_{1} = 1 \cdot 3 + 2$ 3 = 12 + 1  $2 = 2 \cdot (+)$ 

Algorithm 1: ExtendedEuclid(a, b)Input: (a, b) s.t  $a > b \ge 0$ Output: (x, y) s.t. ax + by = gcd(a, b)1 if  $a \mod b = 0$  then2 | Return (0, 1)3 else4 |  $(x, y) \leftarrow ExtendedEuclid (b, a \mod b)$ 5 | Return  $(y, x - y(\lfloor a/b \rfloor))$ 

GCD (6809,1641) 6809 = 47.1641 + 245 (-643, 2668)GCD(1641, 245) 1641 = 6-245 + 171 (96,643 GCD(245, 171)  $245 = \sqrt{(71 + 74)} (-67,96)$ GCD(171, 74) 171= 2.74 + 23 (29,-67) (-9, 2 - -9.3) = (-9, 29) 77 = 3.23 + 5 (-9, 29)GCD(74, 23) (2, -1 - 2.4) = (2, -9) (2, -9) (2, -9)GCD(23, 5) (-1, 1-(-1, 1) = (-1, 2)  $5_{1} = (-1, 2)$   $5_{2} = (-1, 2)$ GCD(5, 3)  $(1, 0 - 1 \times 1) = (1, -1) = 3 = 12 + 1$ GCD(3, 2) (1, -1)GCD(2, 1) (0,1) $2 = 2 \cdot 1 + 0$  (0.1)

#### 9,x- y. [a/b] Greatest Common Divisor GCD (6809, 1641) (-643, 2668) 6809 = 4.1641 + 2451641 = 6-245 + 171 GCD(1641, 245) (96, -643)245=1.171 + 74 GCD(245, 171) (-67, 96)(29, -67)GCD(171, 74) 171=2.74+23 GCD(74, 23) (-9, 2-(-9, 3)) = (-9, 29)77=3:23 + 5 GCD(23, 5) (2, -1 - 2, 4) = (2, -9)23 = 4.5 + 3 GCD(5,3) $(-1, (-(\cdot))) = (-1, 2)$ $5_{1} = 1 \cdot 3 + 2$ GCD(3, 2) (1, $0 - 1 \times 1$ ) = (1 - 1)3 = [12 + 1 $2 = 2 \cdot 1 + 0$ GCD(2, 1) (0,1)

GCD (6809, 1641)  $6809 \times + 1641 \cdot y = 1$  GCD allows us to compute modular inverses.

6809\*(-643) + 1641\*2668 = 1 = GCO(6809/1691) -4,378,187 + 4,378,188 = 1  $1641 \cdot 2688 = 1 + 643 \cdot 6809 \equiv 1 \mod 6809$ 

=> 268B is the "inverse" of 1641 mid 6809.

 $\times 3 \times \frac{1}{3}$ 

#### Euler totient



Q(n) = # of positive integers that are  $\leq n$  and relatively prime to n.

$$\phi(n) = \left| \frac{2}{2} \times \left| gcd(x, n) = \right| \text{ and } x \leq n \right| \right|$$

#### Euler totient

 $\phi(15) = 15 - 5 - 3 + 1 = 8 = (3 - 1)(5 - 1)$ 

1 2 2 4 8 8 7 8 9 10 11 12 13 14

"# integers < 15 that are relatively prime to 15"

#### Euler totient

 $\Phi(p) = p - 1$ 



 $\underline{\Phi(n)} = (\underline{p-1})(\underline{q-1})$ 

 $\phi(7) = 6$ 

product of 2 primes if  $n = p \cdot q$ 

 $\phi(77) = (7-1)(1-1)$ = 6.10 60

### Example of groups $(\mathbb{Z}_n, \star) \quad \{a \mid \gcd(a, n) = 1\}$ multiplicative group, mod n



Z\*\_15 = {1,2,4,7,8,11,13,14}

 $|\mathbb{Z}_n^\star| = \Phi(n)$ "Z-starn"

# Euler theorem $\forall a \in \mathbb{Z}_n^{\star}, \ \underline{a}^{\Phi(n)} = 1 \mod n$

7 mod 31 = 1 mod 31

## Examples

 $\phi(31) = 30$  $7^{30} \mod 31 = 1$ 

 $7^{30} = 7^{16} \cdot 7^{8} \cdot 7^{7} \cdot 7^{2}$ 7  $\cdot [0^{14} \cdot [8] = [7640 = [mod 3]]$ 

### Examples f((5) = (3 - 1)(5 - 1) = 9. $2^8 \mod 15 =$

256 mod 15 = 1 b/c 15.17=255

## Implications of Euler

$$a^{10\phi(N)} \mod N = \left(a^{\phi(N)}\right)^{10} \mod N = \left(1\right)^{10} \mod N = \left(1\right)^{10} \mod N = \left(1\right)^{10} \mod N = 1$$

"heart of 
$$a^{k\phi(N)+1} \mod N = \alpha \cdot a^{K\phi(N)} = \alpha \cdot 1 \mod N$$
  
ESA" =  $\alpha \cdot 1 \mod N$ 

$$11^{30^{2021}} \operatorname{mod}_{(show your work)}^{2021} \underbrace{11^{30^{2021}}}_{(show your work)}^{2023} \underbrace{2 \times ercise}_{(show your work)}^{2023}_{(show your work)}^{2023}_{(show your work)}^{2023}_{10^{2021}}_{10^{2021}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{10^{202}}^{202^{2021}}_{202^{202}}^{202^{2021}}_{10^{202}}^{202^{202}}_{202^{202}}^{202^{202}}_{202^{202}}^{202^{202}}_{10^{202}}^{202^{202}}_{202^{20}}^{202^{202}}_{202^{20}}^{202^{20}}_{20$$

Public Secret. Pick N = p\*q where p,q are primes. Pich a random e that is relatively prime to N. - Compute d s.t. e.d = 1 mod Q(N) - Dublic May (N,e) - Secret Med (N,d)

Pick N = p\*q where p,q are primes.

Pick e,d such that  $e \cdot d = 1 \mod \phi(N)$ 

Pick N = p\*q where p,q are primes.

Pick e,d such that  $e \cdot d = 1 \mod \phi(N)$   $\operatorname{Enc}_{N,e}(m) = m^e \mod N$  $\operatorname{Dec}_{N,d}(c) = c^d \mod N$ 

$$Dec(Enc(m)) = (m^{e})^{d} = m^{e \cdot d} \mod N$$
$$= m^{1 + k \cdot \phi(n)} \mod N$$
$$= m$$

Pick N = p\*q where p,q are primes.

Pick e,d such that  $e \cdot d = 1 \mod \phi(N)$   $\operatorname{Enc}_{N,e}(\underline{m}) = \underline{m^e} \mod N$  $\operatorname{Dec}_{N,d}(\underline{c}) = \underline{c^d} \mod N$ 

$$(m^{e})^{d} \mod N = m^{e \cdot d} \mod N$$

$$= m^{1 + K \cdot \phi(n)} \mod N$$

$$= m \cdot m^{K \cdot \phi(n)} \mod N = m \mod N.$$

## Example of Textbook RSA

m=5

$$enc_{\mu}(5) = 5^{7} \mod 143$$
  
= 47

$$PK = (N=143, e=7) SK = (d=103)$$

$$P = (1 \ q = 13) \quad 7 \cdot (03 = 72) = 1 \ mod \ q(m)$$

$$\phi(m) = (1(-1))(13-1)$$

$$= 120$$

$$Dec_{su}(47) = 47^{9} = 47^{103} \mod 143$$
$$= 5$$

Pick N = p\*q where p,q are primes.

Pick e,d such that  $e \cdot d = 1 \mod \phi(N)$ 

 $Enc_{N,e}(m) = m^e \mod N$  $Dec_{N,d}(c) = c^d \mod N$ 

Why is it insecure against IND-CPA attack?

pkcs1.5

### ENC<sub>pk</sub>( $\underline{m}$ ) PICK $\underline{r}$ as a random string with no Os(typically 8 bytes) $c \leftarrow (0||2||r||0||m)^e \mod N$

"PADDING ORACLE" ATTACK AGAINST THIS SCHEME

**RSA-OAEP+** 

$$\begin{array}{l} r \leftarrow U_n \\ s \leftarrow R_1(r) \oplus m \mid\mid R_2(r||m) \\ t \leftarrow R_3(s) \oplus r \\ c \leftarrow f(s||t) \end{array}$$

$$\begin{array}{l} \mathsf{DEC}_{\mathit{sk}}(\mathcal{C}) \end{array}$$

$$R_{1}: \{0,1\}^{k_{0}} \to \{0,1\}^{n}$$
  

$$R_{2}: \{0,1\}^{n+k_{0}} \to \{0,1\}^{k_{1}}$$
  

$$R_{3}: \{0,1\}^{n+k_{1}} \to \{0,1\}^{k_{0}}$$

$$(s = (s_1, s_2), t) \leftarrow f^{-1}(c)$$
  

$$r \leftarrow R_3(s) \oplus t$$
  

$$m \leftarrow R_1(r) \oplus s_1$$
  

$$R_2(r||m) \stackrel{?}{=} s_2$$
 OUTPUT *m* ELSE FAIL

## Example: apple.com

www.apple.com

Apple Public EV Server RSA CA 2 - G1 DigiCert High Assurance EV Root CA

### Subject Name

Business Category	Private Organization
Inc. Country	US
Inc. State/Province	California
Serial Number	C0806592
Country	US
State/Province	California
Locality	Cupertino
Organization	Apple Inc.
Common Name	www.apple.com

#### Issuer Name

Country US Organization Apple Inc. Common Name <u>Apple Public EV Server RSA CA 2 - G1</u>

### Validity

 Not Before
 Fri, 23 Aug 2024 17:30:11 GMT

 Not After
 Thu, 21 Nov 2024 17:40:11 GMT

com

m.cn

### Subject Alt Names

DNS Name	www.apple.co
DNS Name	images.apple.
DNS Name	www.apple.co

#### Public Key Info

Algorithm RSA Key Size 2048 Exponent 65537 Modulus C8:42:02:8A:C1:1C:A7:9A:EE:58:49:9B:10:3C:41:8D:BF:EF:6F:23:7E:64:05...



### Safari is using an encrypted connection to www.apple.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.

DigiCert, Inc. has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.

### 🛅 DigiCert High Assurance EV Root CA

- L→ 📴 DigiCert SHA2 Extended Validation Server CA-3
  - 🖵 🖂 www.apple.com

Serial Number 03 8E 3F 9E 09 D7 ED C7 B1 80 3F 74 A7 4C 35 AB Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11) Parameters None

Not Valid Before Tuesday, October 6, 2020 at 8:00:00 PM Eastern Daylight Time Not Valid After Friday, October 8, 2021 at 8:00:00 AM Eastern Daylight Time

### Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Parameters None

 
 Public Key
 256 bytes : CA 1B 1C 2178 15 3D 40 CF A3 79 3F 9D CF B2 53 AB A9 41 FF 3E 06 A1 29 69 8A 04 46 9E FB C4 0D 56 7A CA E6 80 C7 AF C6 C0 BF 8B 60 71 CA 9A E8 76 0C 06 C8 9B 77 B8 F3 1B EA 7E E7 3A 84 CB A3 88 A5 93 04 3F 69 66 77 CF AE 06 D1 D9 E1 10 08 7A E0 24 98 E7 56 97 0F 73 68 7B 4D 69 46 28 26 FF 05 81 0C C0 DA FC 21 71 81 65 9A 39 C9 E9 68 36 36 02 5F 81 80 B7 7E 8A 6B FE 34 D0 CE 76 2D D9 8B 3E D4 13 C0 EC EB 0F 2C 77 AD 1E 7B 20 F6 DA 92 98 FD 89 F3 A7 CB 53 16 2E B0 B9 62 BE C8 C3 28 40 CF 8C 5C 61 77 8F 92 3D 2F 23 F2 0A AB 65 82 22 B8 98 CE BA C8 00 95 E4 67 34 6E 76 E5 D1 D3 2D 51 91 BC EF C0 C8 DE F8 7B CC 46 45 00 76 D9 CB 30 31 E9 56 FD 0E 68 F4 36 F9 1B 5F 88 61 62 8F 60 A8 DE 43 7B 5C C1 15 73 D4 06 12 6E 85 9B 50 9C 24 BF 5F FC F4 68 95 67 D5 BF 44 71

 Exponent
 65537

Kev Size 2.048 bits

Hide Certificate

?

OK