The Public Private Key Pair

Edward Curren

@EdwardCurren http://www.edwardcurren.com

Overview

What are asymmetric keys?

The math of key pairs

Where we store these keys

Generate key pairs

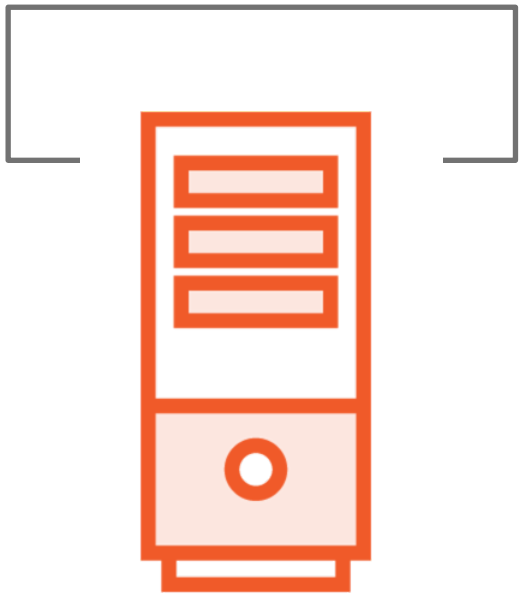
v8f!bLFYt5$z2S%rN#r

v8f!bLFYt5$z2S%rN#r

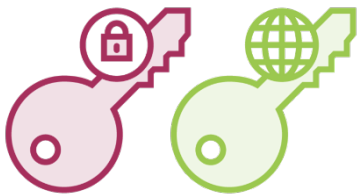
v8f!bLFYt5$z2S%rN#r

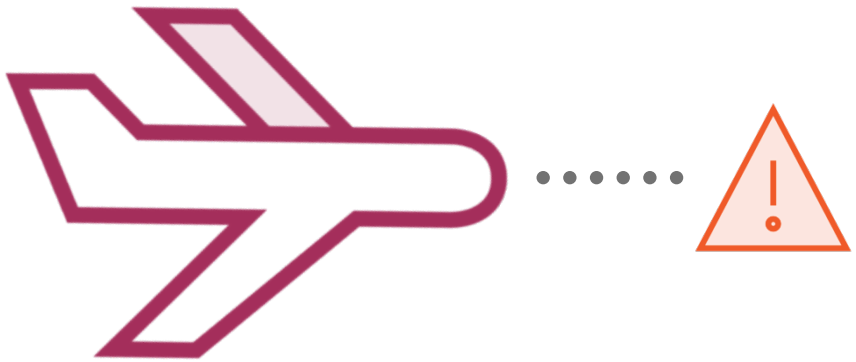
v8f!bLFYt5$z2S%rN#r

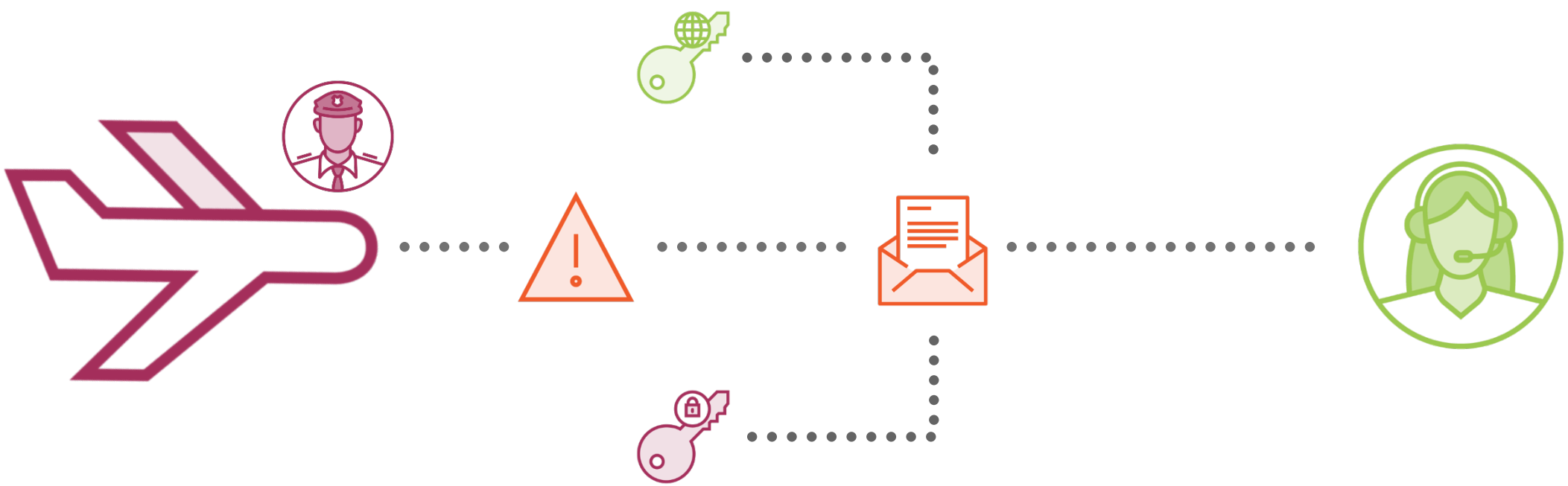
v8f!bLFYt5$z2S%rN#r

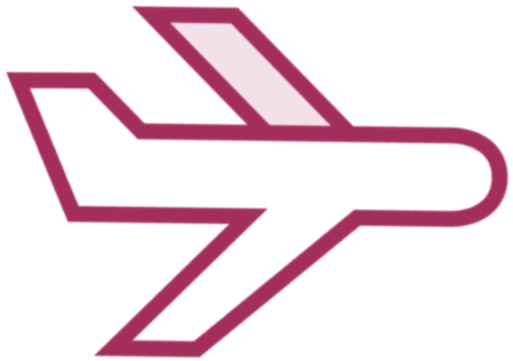


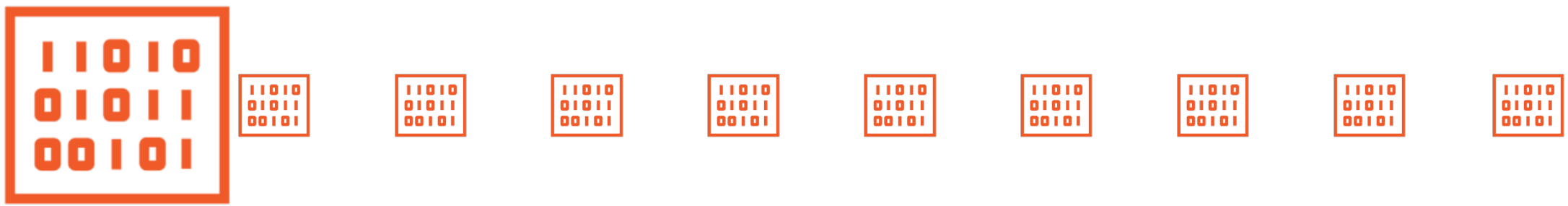

v8f!bLFYt5$z2S%rN#r

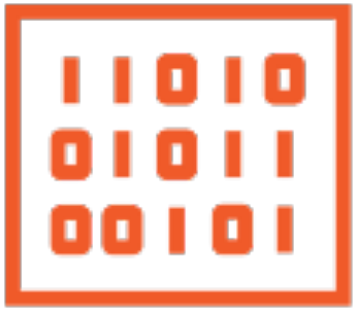












2048 bit key = 245 byte data chunk

Chunk is padded and grows to 256 bytes

1 MB of data transmits 1,045,000 bytes

Order of transmitted data is not assured

ABCDEFG

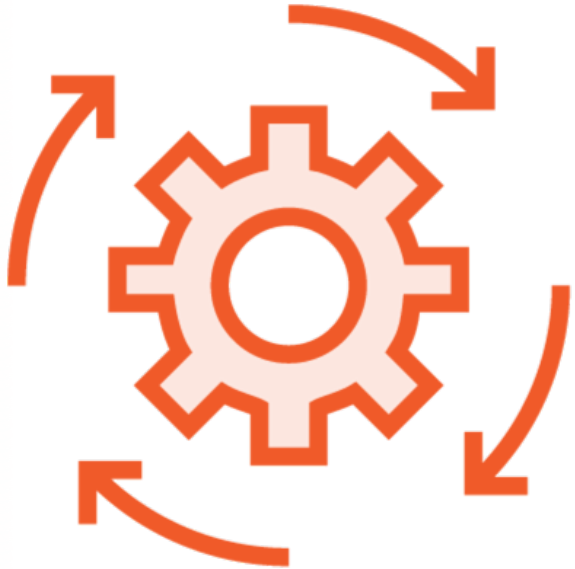
@$&(^%#!^*

ABCDEFG

Discrete Logarithm Problem

1284274223

9284280713



Discrete Logarithm Problem

Six Variables

p Large prime number	**q** Large prime number	**n** Modulus
φ totient(n)	**e** Encryption exponent	**d** Decryption exponent

Filling in the Values

p

148894445742041325547806458
472397916603026273992795 8...

q

527128942521323936106447531 0
309971132180337174752834401 4

...

%

Filling in the Values

p	p = 3
q	q = 11
%	n = 33

Filling in the Values

φ

e

d

Filling in the Values

Filling in the Values

Filling in the Values

φ	$\varphi(n) = 20$
e	
d	

Filling in the Values

φ	$\varphi(n) = 20$
e	
d	

Filling in the Values

φ	$\varphi(n) = 20$
e	$e = 17$
d	

Filling in the Values

φ	$\varphi(n) = 20$
e	$e = 17$
d	

Filling in the Values

φ	$\varphi(n) = 20$
e	$e = 17$
d	

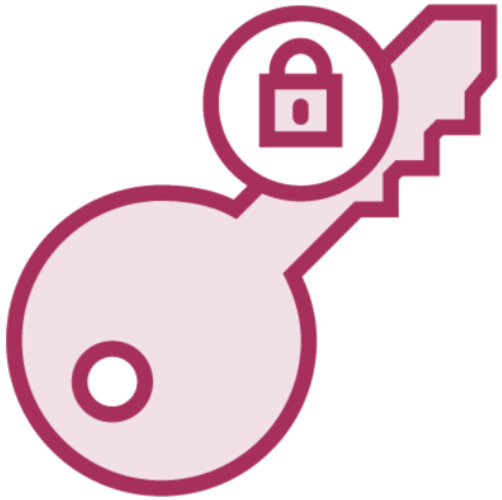
-

Filling in the Values

φ	$\varphi(n) = 20$
e	$e = 17$
d	$d = 13$

Public and Private Keys

Public Key: (e, n)



Private Key: (d, n)

$$m^e \ mod \ n = c$$

$$72^{17} \ mod \ 33 = 30$$

$$c^d \ mod \ n = m$$

$$30^{13} \ mod \ 33 = 6$$

Encryption of “H” with our key pair.

p = 3	q = 11	n = 33
φ(n) = 20	e = 17	d = 13

$$m^e \ mod \ n = c$$
$$13^{17} \ mod \ 33 = 7$$

$$c^d \ mod \ n = m$$
$$7^{13} \ mod \ 33 = 13$$

Encryption of "↲" with our key pair.

p = 3	q = 11	n = 33
φ(n) = 20	e = 17	d = 13

$$m^e \ mod \ n = c$$

$$72^{11} \ mod \ 323 = 98$$

$$c^d \ mod \ n = m$$

$$98^{131} \ mod \ 33 = 72$$

Encryption of “H” with our new key pair.

p = 17	q = 19	n = 323
φ(n) = 288	e = 11	d = 131

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$m^e \ mod \ n = c$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$m^e \ mod \ n = c$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$72^{17} \; mod \; 33 = 30$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$m^e \ mod \ n = c$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$c^d \bmod n = m$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$30^{13} \; mod \; 33 = 6$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$13^{17} \, mod \, 33 = 7$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$7^{13}\ mod\ 33 = 13$$

$p = 3, \quad q = 11, \quad n = 33, \quad \varphi(n) = 20, \quad e = 17, \quad d = 13$

$$m^e \ mod \ n = c$$

$p = 17, \quad q = 19, \quad n = 323, \quad \varphi(n) = 288, \quad e = 11, \quad d = 131$

$$72^{11} \; mod \; 323 = 98$$

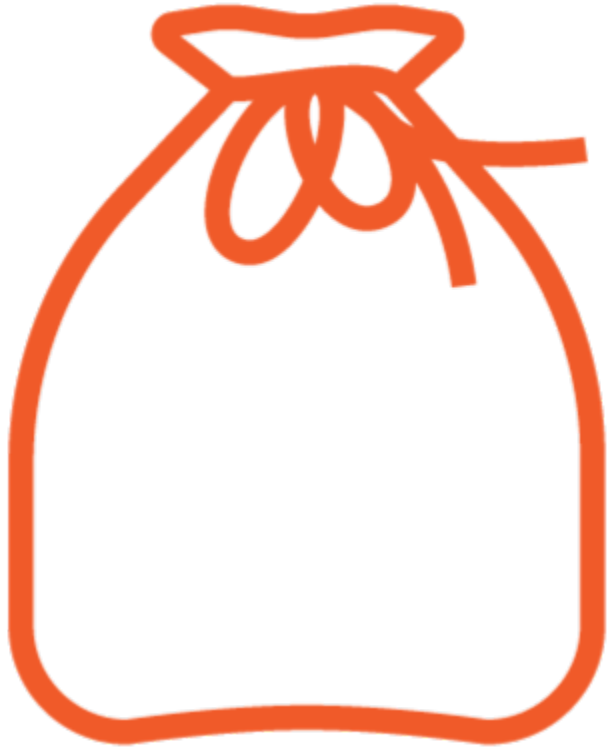
$p = 17, \quad q = 19, \quad n = 323, \quad \varphi(n) = 288, \quad e = 11, \quad d = 131$

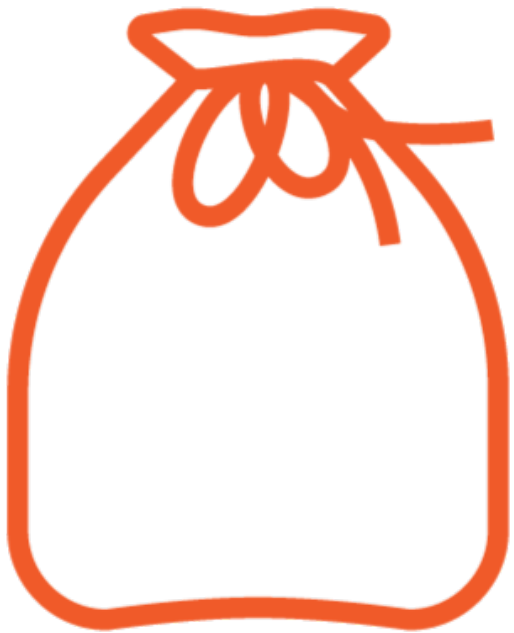
$$98^{131} \; mod \; 323 = 72$$

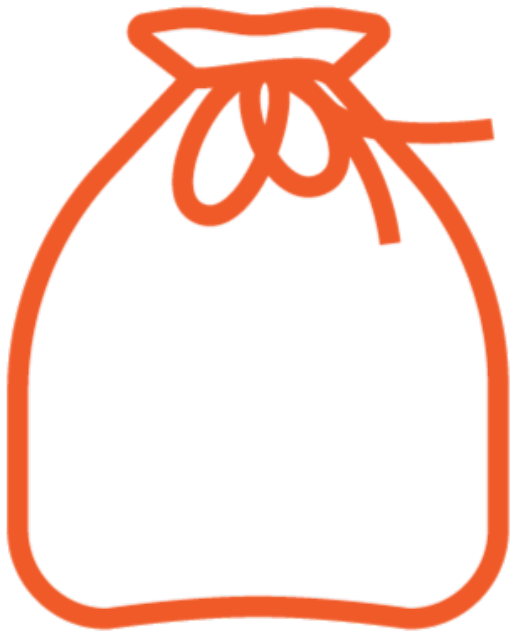
PKCS#12

PKCS#11 and PKCS#15

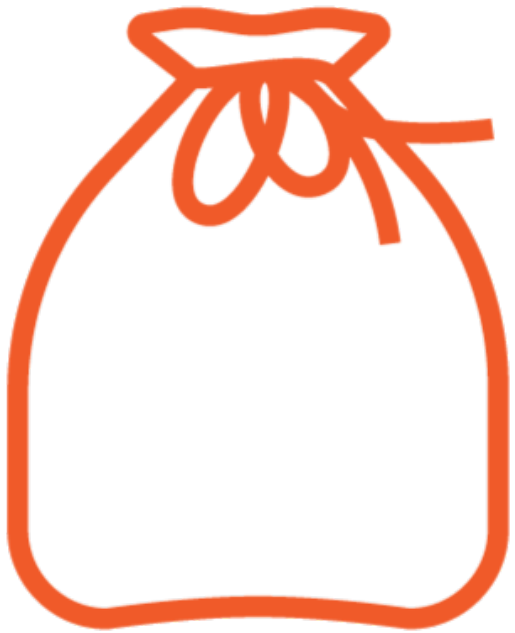
Safe Bag





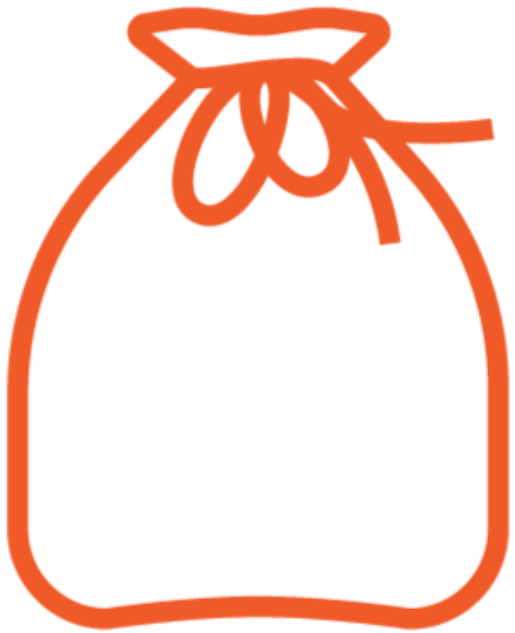


Private Key	• Key Bag • PKCS8 Shrouded Key Bag
Certificates	• Cert Bag
Certificate Revocation List	• CRL Bag
User Defined Data	• Secret Bag



Private Key	• Key Bag • PKCS8 Shrouded Key Bag
Certificates	• Cert Bag
Certificate Revocation List	• CRL Bag
User Defined Data	• Secret Bag


Safe Contents
Private Key
• Key Bag
• PKCS8 Shrouded Key Bag
Certificates
• Cert Bag
Certificate Revocation List
• CRL Bag
User Defined Data
• Secret Bag



Certificate Signing Request

(OID) 1.2.840.113549.1.12.4...

Signing Certificate

(OID) 1.2.840.113549.1.12.4...

Encryption Certificate

(OID) 1.2.840.113549.1.12.4...

Certificate Chain

(OID) 1.2.840.113549.1.12.4...

Summary

Deep dive on the concepts

Will be generating keypairs in the project