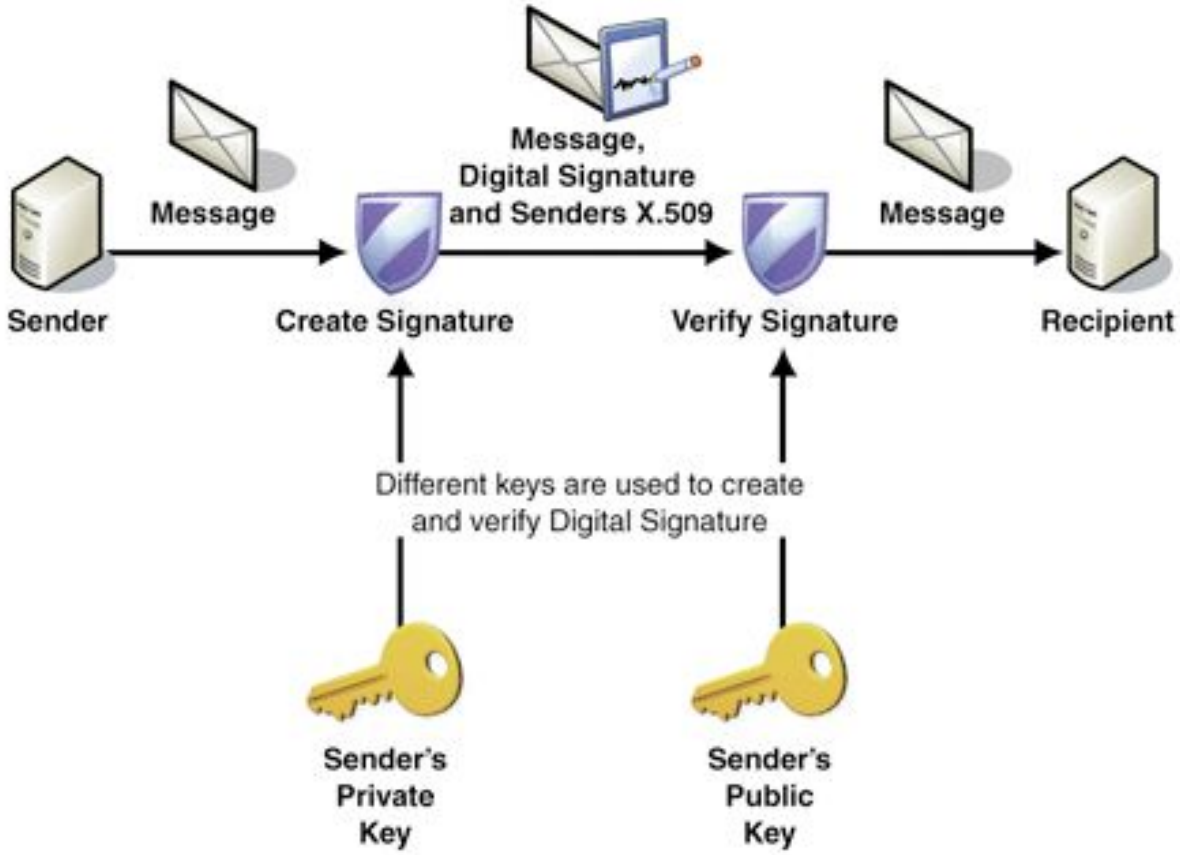
Week 6

Digital Signature



Question 1

Bob generate keys

Selects two prime numbers:
p = 113, q = 89

Calculates the following:
n = p * q
= 113 * 89 = 10057

ϕ(n) = (p - 1) * (q - 1)
= 112 * 88 = 9856

Choose a prime number e co-prime to ϕ(n):
gcd(e, 9856) = 1, 1 < e < ϕ(n)
e = 29

The public key:
(e, n) = (29, 10057)

Calculates the private key d:
de = 1 mod ϕ(n) = e^{-1} mod ϕ(n)
=> d is the multiplicative inverse of e mod ϕ(n)
=> d is the multiplicative inverse of 29 mod 9856
=> d = 7477

Message **m = 500**

Calculates the signature
s = m^d mod n
= 500^{7477} mod 10057 = 8065

Sends **(m, s) = (500, 8065)** to Alice

Alice

Receives public key from Bob:
(e, n) = (29, 10057)

Receives the message and signature from Bob:
(m, s) = (500, 8065)

Verifies Bob's signature using Bob's public key:
m' = s^e mod n
= 8065^{29} mod 10057 = 500

m = m'
=> the message is verified that it came from Bob

Question 2

Bob generate keys

Selects two prime numbers:
p = 131, q = 97

Calculates the following:
n = p * q
= 131 * 97 = 12707

ϕ(n) = (p - 1) * (q - 1)
= 130 * 96 = 12480

Choose a prime number e co-prime to ϕ(n):
gcd(e, 12480) = 1, 1 < e < ϕ(n)
e = 11

The public key:
(e, n) = (11, 12707)

Calculates the private key d:
de = 1 mod ϕ(n) = e^{-1} mod ϕ(n)
=> d is the multiplicative inverse of e mod ϕ(n)
=> d is the multiplicative inverse of 11 mod 12480
=> d = 10211

Message **m = 1234**

Calculates the signature
s = m^d mod n
= 1234^{10211} mod 12707 = 6313

Sends **(m, s) = (1234, 6313)** to Alice

Alice

Receives public key from Bob:
(e, n) = (11, 12707)

Receives the message and signature from Bob:
(m, s) = (1234, 6313)

Verifies Bob's signature using Bob's public key:
m' = s^e mod n
= 6313^{11} mod 12707 = 1234

m = m'
=> the message is verified that it came from Bob

Question 3

Bob generates key

Bob (receiver) chooses
p = 8081, g = 2849, x = 53

Bob calculates:
$y = g^x \bmod p$
$= 2849^{53} \bmod 8081 = 6291$

Bob sends to Alice the public key
p = 8081, g = 2849, y = 6291

Bob signs message **m = 37**

Selects a random number **k, 1 <= k <= p -2**
=> 1 <= k <= 8079
and gcd(k, p - 1) = 1

Picks **k = 11**, which is in the range [1, 8079]
and gcd(11, 8080) = 1, satisfy the condition above.

Computes the signature parameter:
$r = g^k \bmod p$
$= 2849^{11} \bmod 8081 = 1158$

$s = k^{-1} (m - x * r) \bmod (p - 1)$
$= 11^{-1} * (37 - 53 * 1158) \bmod 8080$
$= 11^{-1} * 3303 \bmod 8080$
= 3303 mod 8080 * multiplicative inverse of 11 mod 8080
= 3303 * 6611 mod 8080 = 3973

Sends the signed message to Alice
m = 37, r = 1158, s = 3973

Alice verifies the signature

Receives public key parameters
p = 8081, g = 2849, y = 6291

Receives a signed message
m = 37, r = 1158, s = 3973

Checks if r in the range **[1, p - 1]**
=> 1 <= 1158 <= 8080
=> accepts signature

Computes verification parameters
$v = g^m \bmod p$
$= 2849^{37} \bmod 8081 = 1874$

$w = y^r * r^s \bmod p$
$= 6291^{1158} * 1158^{3973} \bmod 8081 = 1874$

v = w = 1874, signature is accepted

Question 4

Bob generates key

Bob (receiver) chooses
p = 83, g = 79, x = 29

Bob calculates:
$y = g^x \bmod p$
$= 79^{29} \bmod 83 = 15$

Bob sends to Alice the public key
p = 83, g = 79, y = 15

Bob signs message **m = 23**

Selects a random number **k, 1 <= k <= p -2**
=> 1 <= k <= 81
and gcd(k, p - 1) = 1

Picks **k = 11**, which is in the range [1, 81]
and gcd(11, 82) = 1, satisfy the condition above.

Computes the signature parameter:
$r = g^k \bmod p$
$= 79^{11} \bmod 83 = 18$

$s = k^{-1} (m - x * r) \bmod (p - 1)$
$= 11^{-1} * (23 - 29 * 18) \bmod 82$
$= 11^{-1} * (-499) \bmod 82$
$= 11^{-1} * 75 \bmod 82$
= 75 mod 82 * multiplicative inverse of 11 mod 82
$= 75 * 15 \bmod 82 = 59$

Sends the signed message to Alice
m = 23, r = 18, s = 59

Alice verifies the signature

Receives public key parameters
p = 83, g = 79, y = 15

Receives a signed message
m = 23, r = 18, s = 59

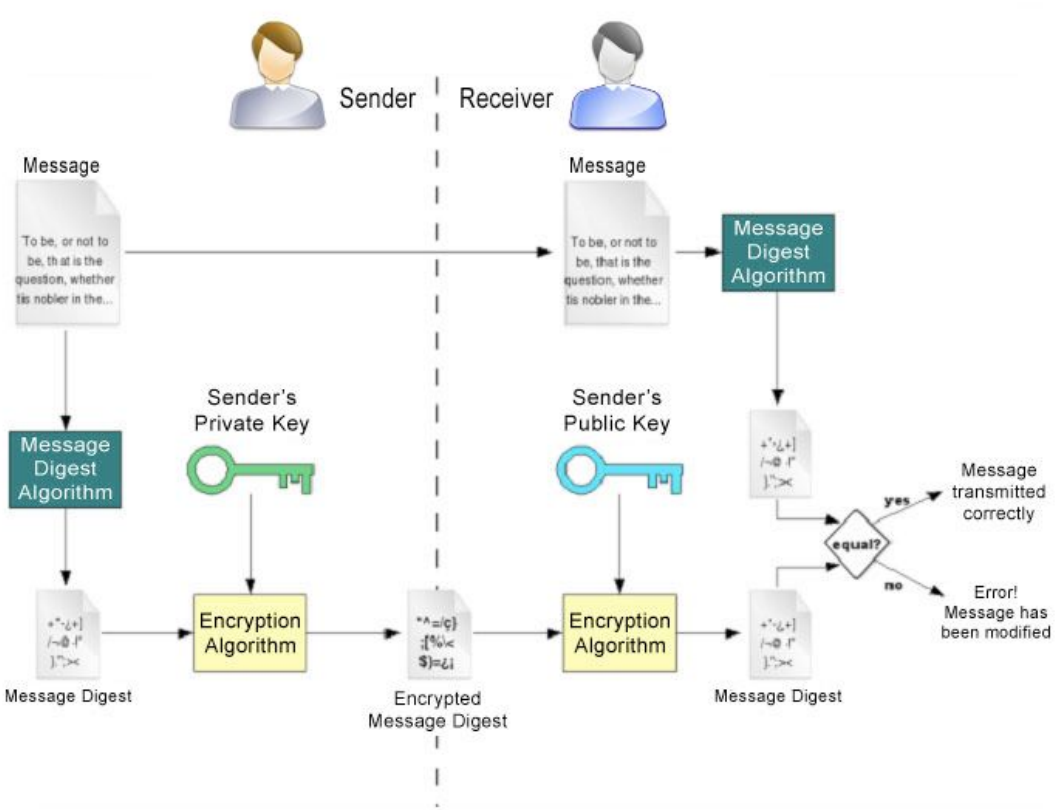
Checks if r in the range **[1, p - 1]**
=> 1 <= 18 <= 82
=> accepts signature

Computes verification parameters
$v = g^m \bmod p$
$= 79^{23} \bmod 83 = 32$

$w = y^r * r^s \bmod p$
$= 15^{18} * 18^{59} \bmod 83 = 32$

v = w = 32, signature is accepted

Digital Signature Complete Scheme



Click here for an example of signing a larger file with the use of hash function

OpenSSL Instructions

Run OpenSSL on Windows: https://youtu.be/Ts-gBfAW28c

On Mac, OpenSSL already installed, just open Terminal app, and type openssl, enter.

Using OpenSSL to generate RSA Private Key and Public Key

https://drive.google.com/file/d/1tBALzGyIT8THdvcFIMbNngWWr4A9z6No/view?usp=sharing

Sign and verify a message:

https://drive.google.com/file/d/1fZWBhIrkdVrWvOU44q92nJ_A1CUHMgbJ/view?usp=sharing

Practical Task

Run openssl command

$ openssl

Generate a private key and store that private key on computer in plaintext

OpenSSL> genrsa -out private.key 2048

Generate the public key from the private key

OpenSSL> rsa -in private.key -pubout -out public.key

Hash a file and sign that file using the private key:

OpenSSL> dgst -sha256 -sign private.key -out sign.sha256 plaintext.txt

Verify the message:

OpenSSL> dgst -sha256 -verify public.key -signature sign.sha256 plaintext.txt

If the message is verified successfully, the following message will apear:

Verified OK

Link to Slides

https://tinyurl.com/y834cjxt