Chapter 2: Cryptography Basics
2.3. Elliptic Curve Cryptography

R. Ziaur, PhD

Outline

- Elliptic Curves over R
- Elliptic Curves over GF(p)
- Computing Point Multiples on Elliptic Curves
- ECDLP
- ECDSA

Elliptic curves over R

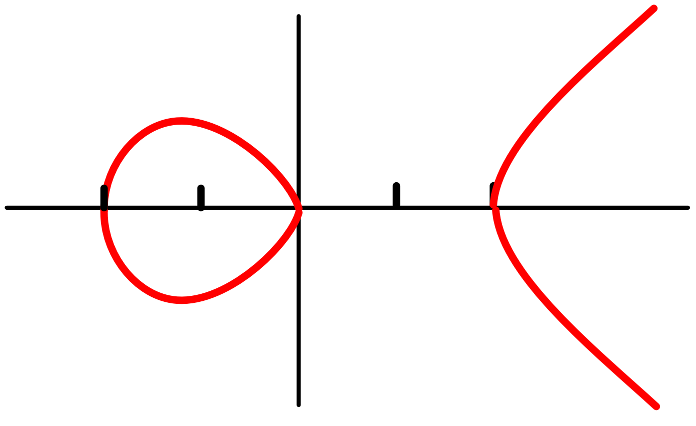
- Definition

Let $a, b \in \boldsymbol{R},\ 4a^3 + 27b^2 \neq 0$

$$E = \left\{ (x, y) \in \boldsymbol{R} \times \boldsymbol{R} \,\middle|\, y^2 = x^3 + ax + b \right\} \cup \{ O \}$$

- Example:

$$E : y^2 = x^3 - 4x$$



Group Operation +

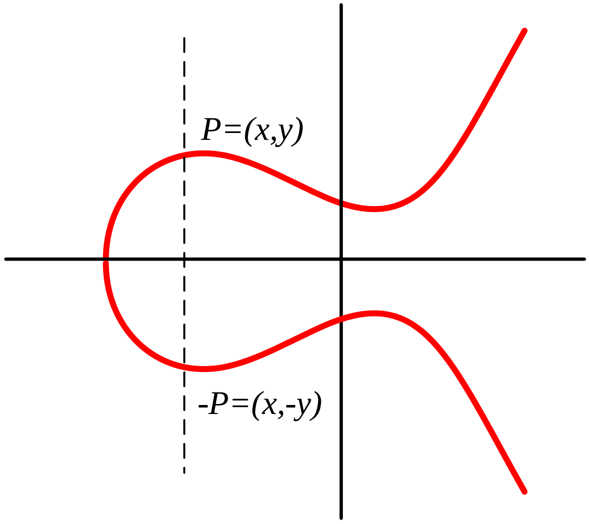
- The point of infinity, O, will be the identity element Given

$$P + O = O + P$$

$$P, Q \in E, P = (x_1, y_1), Q = (x_2, y_2)$$

If $x_1 = x_2$, and $y_1 = -y_2$, then $P + Q = O$

(i.e. $-P = -(x_1, y_1) = (x_1, -y_1)$)



Group operation +

Given $P, Q \in E, P = (x_1, y_1), Q = (x_2, y_2)$

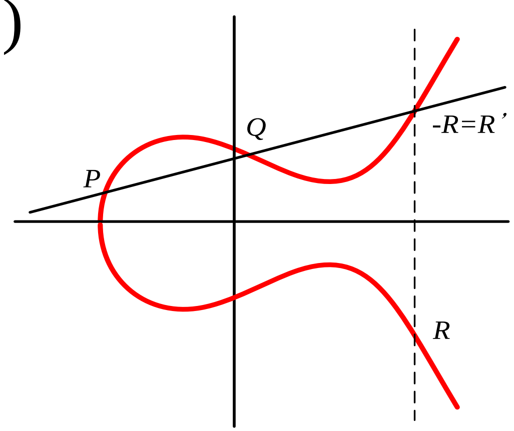
Compute $R = P + Q = (x_3, y_3)$

– Addition $(P \neq Q)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$

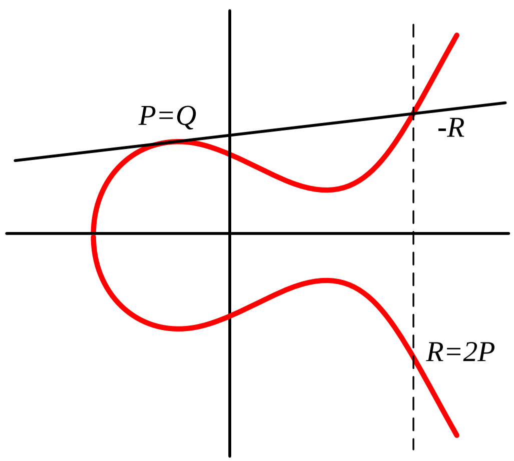


– Doubling $(P = Q)$

$$\lambda = \frac{3x_1^{\ 2} + a}{2y_1}$$

$$x_3 = \lambda^2 - 2x_1$$

$$y_3 = (x_1 - x_3)\lambda - y_1$$



Example (addition):

- Given
  - $E: y^2 = x^3 - 25x$

$P = (x_1, y_1) = (0,0),\ \ Q = (x_2, y_2) = (-5,0),\ \ P + Q = (x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{0-0}{-5-0} = 0$$

$$x_3 = \lambda^2 - x_1 - x_2 = 0^2 - 0 - \left(-5\right) = 5$$

$$y_3 = (x_1 - x_3)\lambda - y_1 = \left(0-5\right) \times 0 - 0 = 0$$

Example (doubling)

Given

- $E : y^2 = x^3 - 25x$

  $P = (x_1, y_1) = (-4,6),\ \ 2P = (x_2, y_2)$

$$\lambda = \frac{3x_1^{\ 2} + a}{2y_1} = \frac{3(-4)^2 - 25}{2 \times 6} = \frac{23}{12}$$

$$x_2 = \lambda^2 - 2x_1 = \left(\frac{23}{12}\right)^2 - 2 \times (-4) = \frac{1681}{144}$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = \left(-4 - \frac{1681}{144}\right) \times \frac{23}{12} - 6 = -\frac{62279}{1728}$$

Elliptic Curves over GF(p)

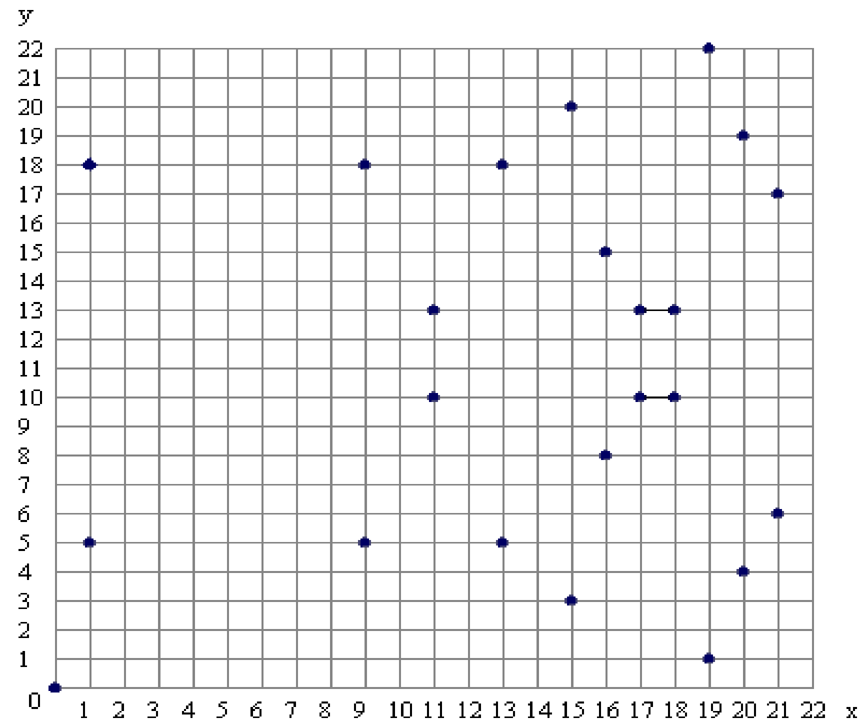
- Definition

Let $p > 3, a, b \in Z_p,\ 4a^3 + 27b^2 \neq 0 \pmod{p}$

$$E = \left\{ (x, y) \in Z_p \times Z_p \,\middle|\, y^2 \equiv x^3 + ax + b \pmod{p} \right\} \cup \{ O \}$$

$E : y^2 = x^3 + x$ over Z_{23}

- Example:



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

Galois Field GF(p)

- p is a prime number
- Example: GF(11)={0,1,2,3,4,5,6,7,8,9,10}
- 13 (mod 11) = 2, 13=24=35=2 (mod 11)
- 8+9=17=6 (mod 11)
- 8-9= -1 =10 (mod 11)
- 3x4=12=1 (mod 11)
- $3/4 = 3\times4^{-1} = 3\times3 = 9$ (mod 11)
- *Multiplicative inverse:*
- *(1,1), (2,6),(3,4),(5,9),(7,8)*

Example

$$E : y^2 = x^3 + x + 6 \text{ over } Z_{11}$$

Find all *(x, y)* and O:

- Fix *x* and determine *y*
- O is an artificial point

12 *(x, y)* pairs plus O,

and have *#E=13*

x	$x^3 + x + 6$	quad res?	y
0	6	*no*	
1	8	*no*	
2	5	*yes*	4,7
3	3	*yes*	5,6
4	8	*no*	
5	4	*yes*	2,9
6	8	*no*	
7	4	*yes*	2,9
8	9	*yes*	3,8
9	7	*no*	
10	4	*yes*	2,9

Example (continue)

- There are 13 points on the group $E(Z_{11})$ and so any non-identity point (i.e. not the point at infinity, noted as O) is a generator of $E(Z_{11})$.

Choose generator $\alpha = (2,7)$
Compute $2\alpha = (x_2, y_2)$

$$\lambda = \frac{3x_1^{\ 2} + a}{2y_1} = \frac{3(2)^2 + 1}{2 \times 7} = \frac{13}{14} = 2 \times 3^{-1} = 2 \times 4 = 8 \mod 11$$

$$x_2 = \lambda^2 - 2x_1 = (8)^2 - 2 \times (2) = 5 \mod 11$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = (2-5) \times 8 - 7 = 2 \mod 11$$

Example (continue)

- Compute $3\alpha = (x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-7}{5-2} = 2 \mod 11$$

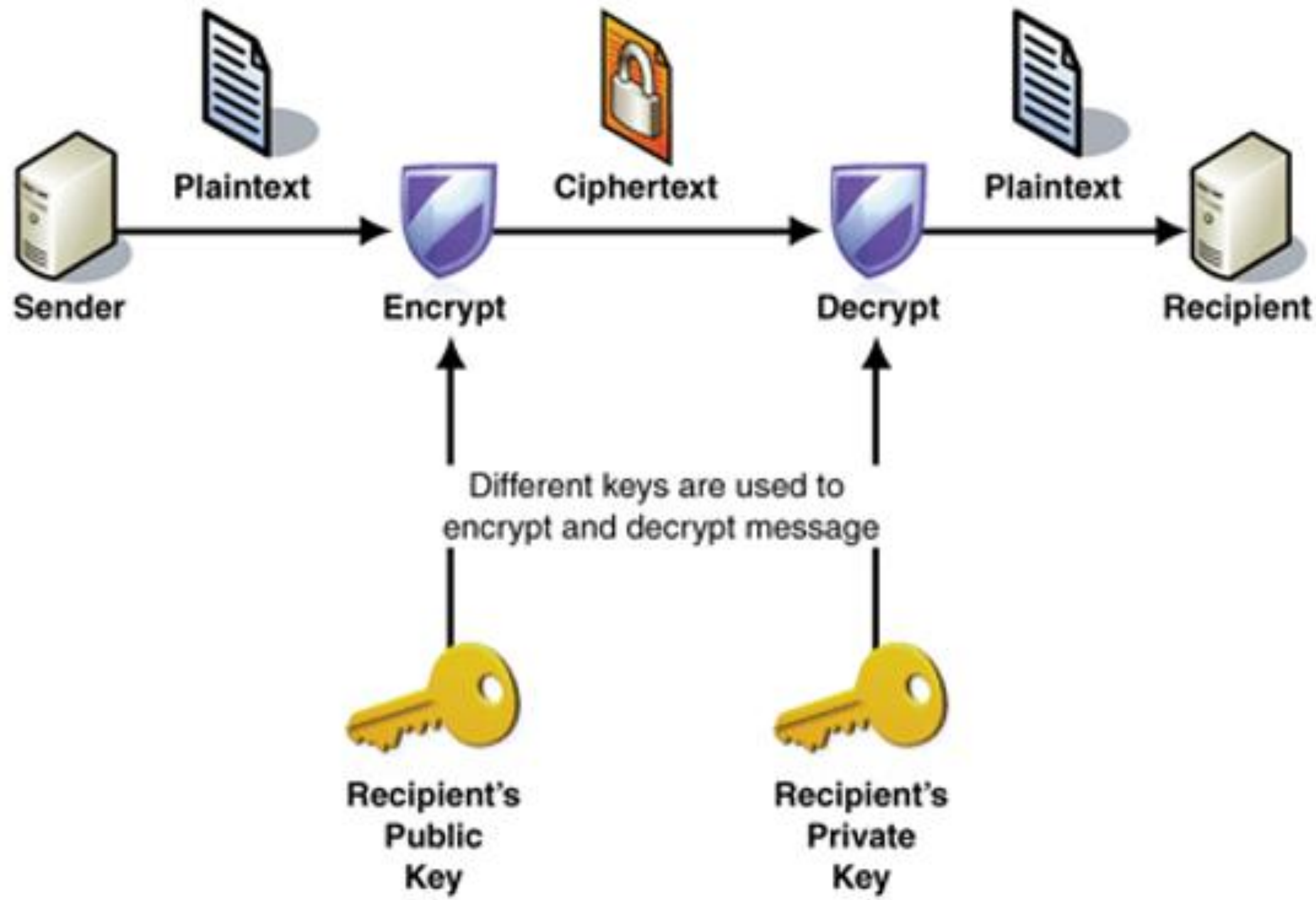
$$x_3 = \lambda^2 - x_1 - x_2 = 2^2 - 2 - 5 = 8 \mod 11$$

$$y_3 = (x_1 - x_3)\lambda - y_1 = (2-8) \times 2 - 7 = 3 \mod 11$$

So, we can compute

$$\begin{array}{lll} \alpha = (2,7) & 2\alpha = (5,2) & 3\alpha = (8,3) \\ 4\alpha = (10,2) & 5\alpha = (3,6) & 6\alpha = (7,9) \\ 7\alpha = (7,2) & 8\alpha = (3,5) & 9\alpha = (10,9) \\ 10\alpha = (8,8) & 11\alpha = (5,9) & 12\alpha = (2,4) \end{array}$$

Public Key Encryption



Example (continue)

- Let's modify ElGamal encryption by using the elliptic curve *E(Z$_{11}$).*
  Suppose that $\alpha = (2,7)$ and Bob's private key is x=7, the public key is

  $$y = x\alpha = 7\alpha = (7,2)$$

  The encryption operation is

  $$e_K(m,k) = \left(k\alpha, m + ky\right) = (k(2,7), m + k(7,2)),$$

  where $x \in E$ and $0 \le k \le 12$, and the decryption operation is

  $$d_K(a,b) = b - 7a.$$

Example (continue)

- Suppose that Alice wishes to encrypt the plaintext m = (10,9) (which is a point on E).
  If she chooses the random value k = 3, then

$$a = 3(2,7) = (8,3) \text{ and}$$

$$b = (10,9) + 3(7,2) = (10,9) + (3,5) = (10,2)$$

  Hence $c = \left((8,3),(10,2)\right)$. Now, if Bob receives the ciphertext c, he decrypts it as follows:

$$m = (10,2) - 7(8,3) = (10,2) - (3,5)$$

$$= (10,2) + (3,6) = (10,9)$$

Computing Point Multiples on Elliptic Curves

- Use Double-and-Add
  (similar to square-and-multiply)
  Algorithm: $(P,(c_{l-1},\ldots,c_0)),\ c_i \in \{0,1\}$
  DOUBLE-AND-ADD

$$
\begin{array}{l}
Q \leftarrow O \\
\text{for } i \leftarrow l-1 \text{ downto } 0 \\
\quad \text{do } \begin{cases} Q \leftarrow 2Q \\ \text{if } c_i = 1 \\ \quad \text{then } Q \leftarrow Q + P \end{cases} \\
\text{return } (Q)
\end{array}
$$

Example

- Compute 7P
- $7P=(2^2+2+1)P=2(2P+P)+P$
- 2 doublings and 2 additions instead of 7 additions

Example

- Compute 3895P

$$3895P = \underbrace{P + P + \cdots + P}_{3894 \text{ additions needed}}$$

$$= (111100110111)_2 P$$

$$= 2(2(2(2(2(2(2(2(2(2(2P + P) + P) + P))) + P) + P)) + P) + P) + P$$

$$\rightarrow 11 \text{ doublings and } 8 \text{ additions needed}$$

Elliptic Curve DLP

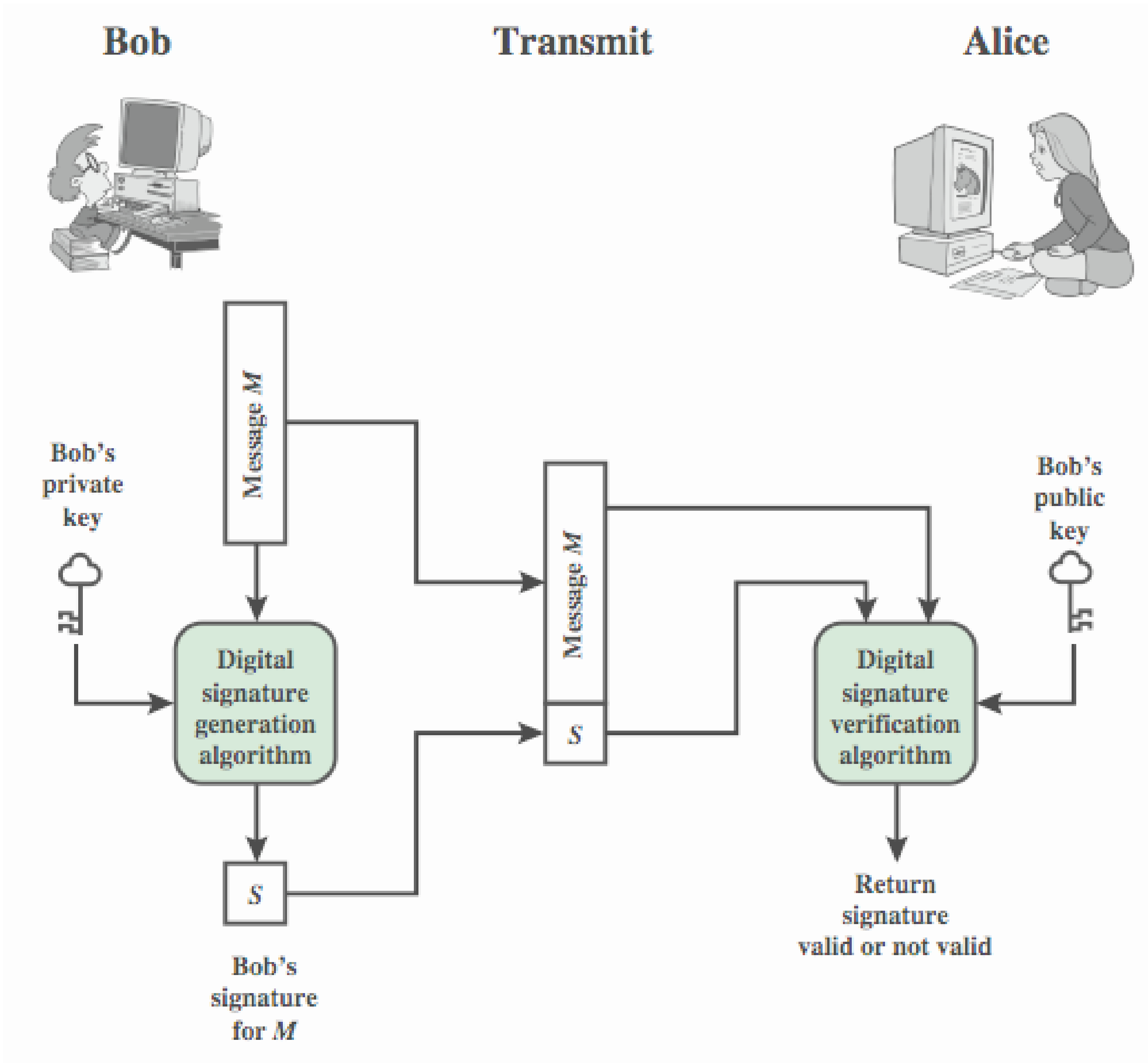
- Basic computation of ECC
  - $Q = kP = \underbrace{P + P + ... + P}_{k\ times}$
    where P is a curve point, k is an integer

- Strength of ECC
  - Given curve, the point P, and kP
    It is hard to recover k
    - Elliptic Curve Discrete Logarithm Problem (ECDLP)

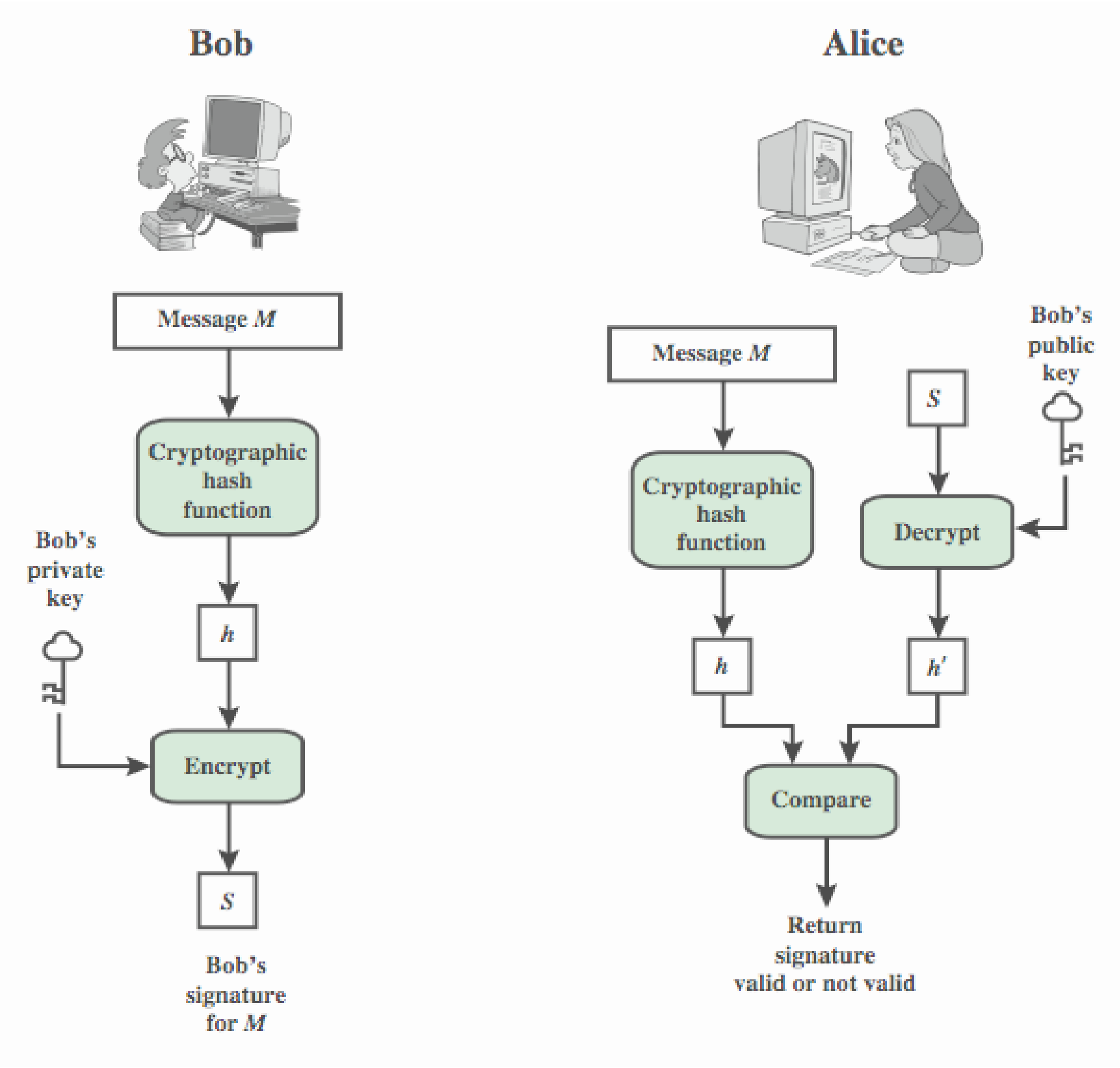
Signature Scheme: ECDSA

- Digital Signature Algorithm (DSA)
  - Proposed in 1991
  - Was adopted as a standard on December 1, 1994
- Elliptic Curve DSA (ECDSA)
  - FIPS 186-2 in 2000

Digital Signature Model



Cont.


Bob
Alice
Message M
Cryptographic hash function
h
Bob's private key
Encrypt
S
Bob's signature for M
Message M
S
Bob's public key
Cryptographic hash function
Decrypt
h
h'
Compare
Return signature valid or not valid

Elliptic Curve DSA

- Let p be a prime, and let E be an elliptic curve defined over GF(p). Let A be a point on E having prime order q, such that DL problem in <A> is infeasible.

  Define *K*={ (p, q, E, A, x, Y): Y=xA }

  p, q, E, A,Y are the public key, x is private

ECDSA

- For a (secret) random number k, define $sig_x(m,k)=(r,s)$,

  where $kA=(u,v)$, $r=u \bmod q$ and

  $s=k^{-1}(Hash(m)+xr) \bmod q$

- For a message $(m,(r,s))$, verification is done by performing the following computations:

  $i=Hash(m) \cdot s^{-1} \bmod q$

  $j=r \cdot s^{-1} \bmod q$

  $(u,v)=iA+jY$

  $ver(m,(r,s))=true$ if and only if $u \bmod q=r$

Elliptic Curve Security

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

NIST Recommended Key Sizes

Security of ECC versus RSA/ElGamal

- Elliptic curve cryptosystems give the most security per bit of any known public-key scheme.
- The ECDLP problem appears to be much more difficult than the integer factorisation problem and the discrete logarithm problem of Z_p.
- The strength of elliptic curve cryptosystems grows much faster with the key size increases than does the strength of RSA.

RSA

- by Rivest, Shamir & Adleman of MIT in 1977
- best known & widely used public-key scheme

http://www.ams.org/notices/200307/comm-turing.pdf

RSA En/decryption

- to encrypt a message M the sender:
  - obtains **public key** of recipient $PU=\{e,n\}$
  - computes: $C = M^e \bmod n$, where $0 \leq M < n$
- to decrypt the ciphertext C the owner:
  - uses their private key $PR=\{d,n\}$
  - computes: $M = C^d \bmod n$
- note that the message M must be smaller than the modulus n (block if needed)

RSA Example - Key Setup

1. Select primes: p=17 & q=11
2. Calculate $n = pq$ =17 x 11=187
3. Calculate $ø(n)=(p–1)(q-1)$=16x10=160
4. Select e: gcd(e,160)=1; choose e=7
5. Determine d: de=1 mod 160 and d < 160
   Value is d=23 since 23x7=161= 10x160+1
6. Publish public key PU={7,187}
7. Keep secret private key PR={23,187}

RSA Example - En/Decryption

- sample RSA encryption/decryption is:
- given message $M = 88$ (nb. $88<187$)
- encryption:

  $C = 88^7 \bmod 187 = 11$

- decryption:

  $M = 11^{23} \bmod 187 = 88$

ECC Benefits

ECC is particularly beneficial for application where:

- computational power is limited (wireless devices, PC cards)
- integrated circuit space is limited (wireless devices, PC cards)
- high speed is required.
- intensive use of signing, verifying or authenticating is required.
- signed messages are required to be stored or transmitted (especially for short messages).
- bandwidth is limited (wireless communications and some computer networks).