# Practical Aspects of Modern Cryptography

Josh Benaloh & Brian LaMacchia

# Lecture 8: EKE, DSA, Elliptic Curves, and Primality Testing

## Encrypted Key Exchange

- We know how Alice and Bob can communicate securely if they share a strong (128-bit) private key or if one has a public key known to the other.
- Suppose that Alice and Bob share only a short (potentially searchable) password.
- Rather than using just this weak password, Alice and Bob can use this weak password to bootstrap a strong key.



## Encrypted Key Exchange

Alice and Bob share weak password P.

Let C be a symmetric cipher agreed upon by Alice and Bob.

- Alice begins by generating a public/private key pair (E,D).
- Alice sends Bob $C_P(E)$.
- Bob generates a random symmetric key K and sends Alice $C_P(E(K))$.



## Encrypted Key Exchange

Alice and Bob can then demonstrate to each other their knowledge of K as an authentication step.

- Alice generates a random nonce A and sends $C_K(A)$ to Bob.
- Bob generates a random nonce B and sends $C_K(A,B)$ to Alice.
- Alice sends $C_K(B)$ to Bob.



## The Digital Signature Algorithm

In 1991, the National Institute of Standards and Technology published a Digital Signature Standard that was intended as an option free of intellectual property constraints.

## The Digital Signature Algorithm

DSA uses the following parameters

- Prime $p$ – anywhere from 512 to 1024 bits
- Prime $q$ – 160 bits such that $q$ divides $p$-1
- Integer $h$ in the range $1 < h < p-1$
- Integer $g = h^{(p-1)/q} \bmod p$
- Secret integer $x$ in the range $1 < x < q$
- Integer $y = g^x \bmod p$



## The Digital Signature Algorithm

To sign a 160-bit message M,

- Generate a random integer $k$ with $0 < k < q$,
- Compute $r = (g^k \bmod p) \bmod q$,
- Compute $s = ((M+xr)/k) \bmod q$.

The pair $(r,s)$ is the signature on M.



## The Digital Signature Algorithm

A signature $(r,s)$ on $M$ is verified as follows:

- Compute $w = 1/s \bmod q$,
- Compute $a = w\text{M} \bmod q$,
- Compute $b = wr \bmod q$,
- Compute $v = (g^a y^b \bmod p) \bmod q$.

Accept the signature only if $v = r$.



## Elliptic Curve Cryptosystems

An elliptic curve

$$y^2 = x^3 + Ax + B$$



## Elliptic Curves

$$y^2 = x^3 + Ax + B$$

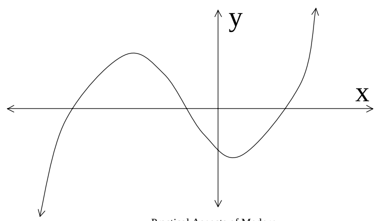


## Elliptic Curves

$$y \;\; = x^3 + Ax + B$$

## Elliptic Curves

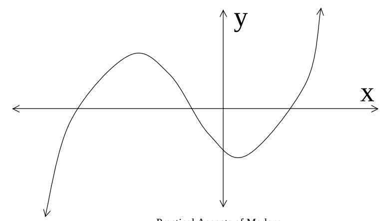
$$y \ \ = x^3 + Ax + B$$






## Elliptic Curves

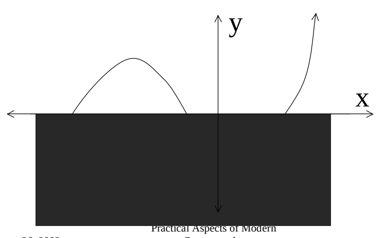
$$y^2 = x^3 + Ax + B$$






## Elliptic Curves

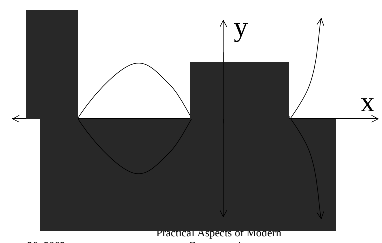
$$y^2 = x^3 + Ax + B$$






## Elliptic Curves

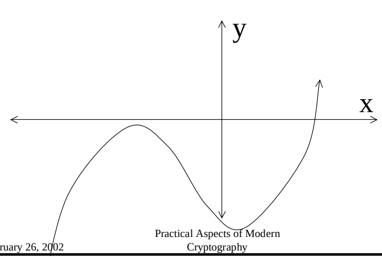
$$y^2 = x^3 + Ax + B$$






## Elliptic Curves

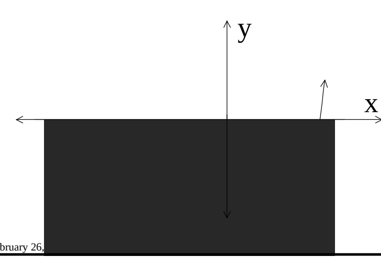
$$y^2 = x^3 + Ax + B$$





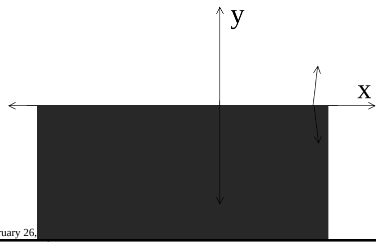

## Elliptic Curves

$$y^2 = x^3 + Ax + B$$



## Elliptic Curves

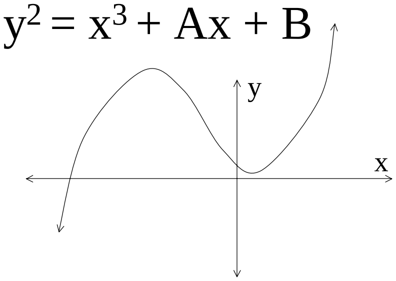
$$y^2 = x^3 + Ax + B$$






## Elliptic Curves

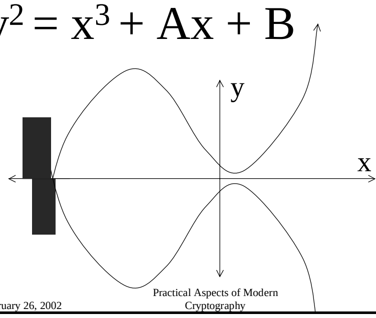
$$y^2 = x^3 + Ax + B$$






## Elliptic Curves

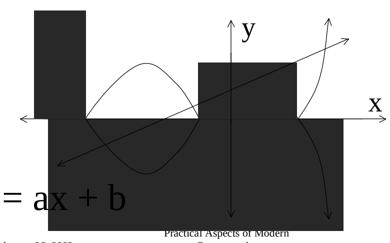
$$y^2 = x^3 + Ax + B$$






## Elliptic Curves Intersecting Lines

$$y^2 = x^3 + Ax + B$$






## Elliptic Curves Intersecting Lines

<u>Non-vertical Lines</u>

$$\begin{cases} y^2 = x^3 + Ax + B \\ y = ax + b \end{cases}$$

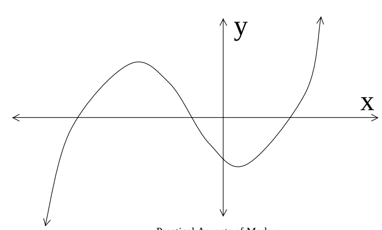
$$(ax + b)^2 = x^3 + Ax + B$$

$$x^3 + A'x^2 + B'x + C' = 0$$



## Elliptic Curves Intersecting Lines

$$x^3 + A'x^2 + B'x + C' = 0$$



## Elliptic Curves Intersecting Lines

Non-vertical Lines

- 1 intersection point (typical case)
- 2 intersection points (tangent case)
- 3 intersection points (typical case)



## Elliptic Curves Intersecting Lines

Vertical Lines

$$\begin{cases} y^2 = x^3 + Ax + B \\ x = c \end{cases}$$

$$y^2 = c^3 + Ac + B$$

$$y^2 = C$$



## Elliptic Curves Intersecting Lines

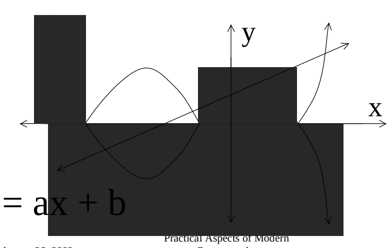
Vertical Lines

- 0 intersection point (typical case)
- 1 intersection points (tangent case)
- 2 intersection points (typical case)



## Elliptic Groups

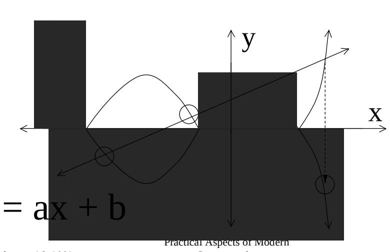
$$y^2 = x^3 + Ax + B$$






## Elliptic Groups

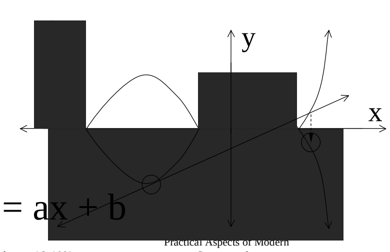
$$y^2 = x^3 + Ax + B$$





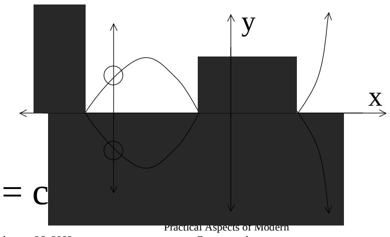

## Elliptic Groups

$$y^2 = x^3 + Ax + B$$



## Elliptic Groups

$$y^2 = x^3 + Ax + B$$




$x = c$



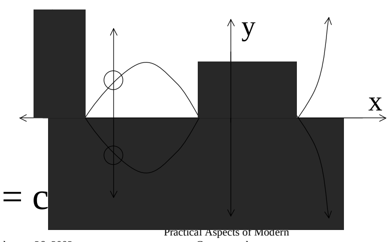
## Elliptic Groups

- Add an “artificial” point I to handle the vertical line case.
- This point I also serves as the group identity value.



## Elliptic Groups

$$y^2 = x^3 + Ax + B$$




$x = c$



## Elliptic Groups

$$(x_1,y_1) \times (x_2,y_2) = (x_3,y_3)$$

$$x_3 = ((y_2-y_1)/(x_2-x_1))^2 - x_1 - x_2$$
$$y_3 = -y_1 + ((y_2-y_1)/(x_2-x_1))\,(x_1 - x_3)$$

when $x_1 \neq x_2$



## Elliptic Groups

$$(x_1,y_1) \times (x_2,y_2) = (x_3,y_3)$$

$$x_3 = ((3x_1^2+A)/(2y_1))^2 - 2x_1$$
$$y_3 = -y_1 + ((3x_1^2+A)/(2y_1))\,(x_1 - x_3)$$

when $x_1 = x_2$ and $y_1 = y_2 \neq 0$



## Elliptic Groups

$$(x_1,y_1) \times (x_2,y_2) = I$$
when $x_1 = x_2$ but $y_1 \neq y_2$ or $y_1 = y_2 = 0$

$$(x_1,y_1) \times I = (x_1,y_1) = I \times (x_1,y_1)$$

$$I \times I = I$$

## The Fundamental Equation

$$Z=Y^X \bmod N$$



## The Fundamental Equation

$$Z=Y^X \text{ in } E_p(A,B)$$



## The Fundamental Equation

$$Z=Y^X \text{ in } E_p(A,B)$$

When Z is unknown, it can be efficiently computed by repeated squaring.



## The Fundamental Equation

$$Z=Y^X \text{ in } E_p(A,B)$$

When X is unknown, this version of the discrete logarithm is believed to be quite hard to solve.



## The Fundamental Equation

$$Z=Y^X \text{ in } E_p(A,B)$$

When Y is unknown, it *can* be efficiently computed by “sophisticated” means.



## Diffie-Hellman Key Exchange

| Alice | Bob |
|---|---|
| ♦ Randomly select a large integer $a$ and send A $= Y^a \bmod N$. | ♦ Randomly select a large integer $b$ and send B $= Y^b \bmod N$. |
| ♦ Compute the key $K = B^a \bmod N$. | ♦ Compute the key $K = A^b \bmod N$. |

$$B^a = Y^{ba} = Y^{ab} = A^b$$

## Diffie-Hellman Key Exchange

| Alice | Bob |
|---|---|
| ♦ Randomly select a large integer *a* and send A = $Y^a$ in $E_p$. | ♦ Randomly select a large integer *b* and send B = $Y^b$ in $E_p$. |
| ♦ Compute the key K = $B^a$ in $E_p$. | ♦ Compute the key K = $A^b$ in $E_p$. |

$B^a = Y^{ba} = Y^{ab} = A^b$



## DSA on Elliptic Curves

- Almost identical to DSA over the integers.
- Replace operations mod *p* and *q* with operations in $E_p$ and $E_q$.



## Why use Elliptic Curves?

- The best *currently known* algorithm for EC discrete logarithms would take about as long to find a 160-bit EC discrete log as the best *currently known* algorithm for integer discrete logarithms would take to find a 1024-bit discrete log.
- 160-bit EC algorithms are somewhat faster and use shorter keys than 1024-bit “traditional” algorithms.



## Why *not* use Elliptic Curves?

- EC discrete logarithms have been studied far less than integer discrete logarithms.
- Results have shown that a fundamental break in integer discrete logs would also yield a fundamental break in EC discrete logs, although the reverse may not be true.
- Basic EC operations are more cumbersome than integer operations, so EC is only faster if the keys are *much* smaller.



## Finding Primes

Euclid’s proof of the infinity of primes

- Suppose that the set of all primes were finite.
- Let N be the product of all of the primes.
- Consider N+1.
- The prime factors of N+1 are not among the finite set of primes multiplied to form N.
- This contradicts the assumption that the set of all primes is finite.



## The Prime Number Theorem

The number of primes less than N is approximately N/(ln N).

Thus, approximately 1 out of every *n* randomly selected *n*-bit integers will be prime.

## Testing Primality

Recall Fermat's Little Theorem

If $p$ is prime, then $a^{(p-1)} \bmod p = 1$ for all $a$ in the range $0 < a < p$.



## The Miller-Rabin Primality Test

To test an integer N for primality, write N-1 as $N-1 = m2^k$ where $m$ is odd.

Repeat several (many) times

- Select a random $a$ in $1 < a < N-1$
- Compute $a^m, a^{2m}, a^{4m}, \ldots, a^{(N-1)/2}$ all mod N.
- If $a^m = \pm 1$ or if some $a^{2^i m} = -1$, then N is probably prime – continue.
- Otherwise, N is composite – stop.



## Sieving for Primes

Pick a random starting point N.

| N | N+1 | N+2 | N+3 | N+4 | N+5 | N+6 | N+7 | N+8 | N+9 | N+10 | N+11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | X | X | X | | X | | X | X | X | X | X |

Sieving out multiples of 5

Only a few "good" candidate primes will survive.