CS 161: Computer Security

Lecture 6

September 17, 2015

Where we are

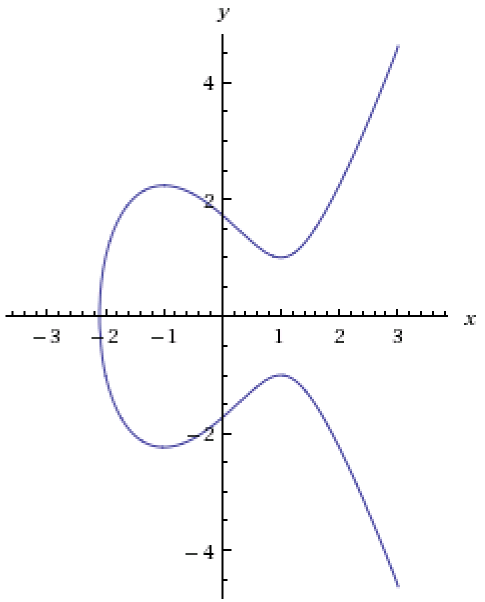
- How did NSA break SSL?
- Basic number theory
- RSA
- Digital certificates
- Shamir secret sharing
- Rabin signatures
- Secure hashing
- Elliptic curve cryptography
- Pseudo-random number generation
- SSL protocol

This lecture

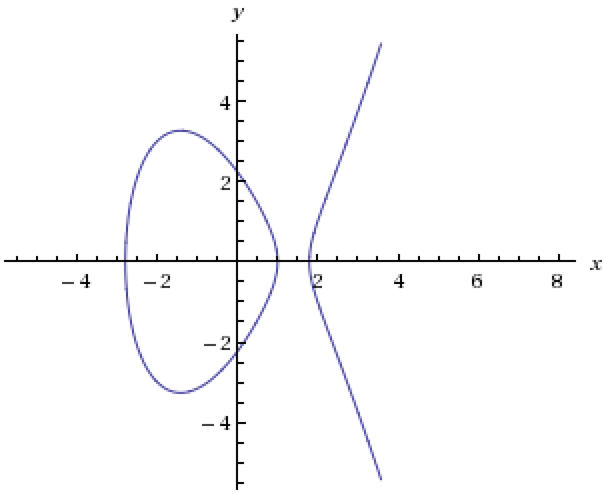
- Elliptic curve cryptography
- Pseudo random number generation

Review: Elliptic curves

- Weierstrass equations
- $y^2 = x^3 + Ax + B$

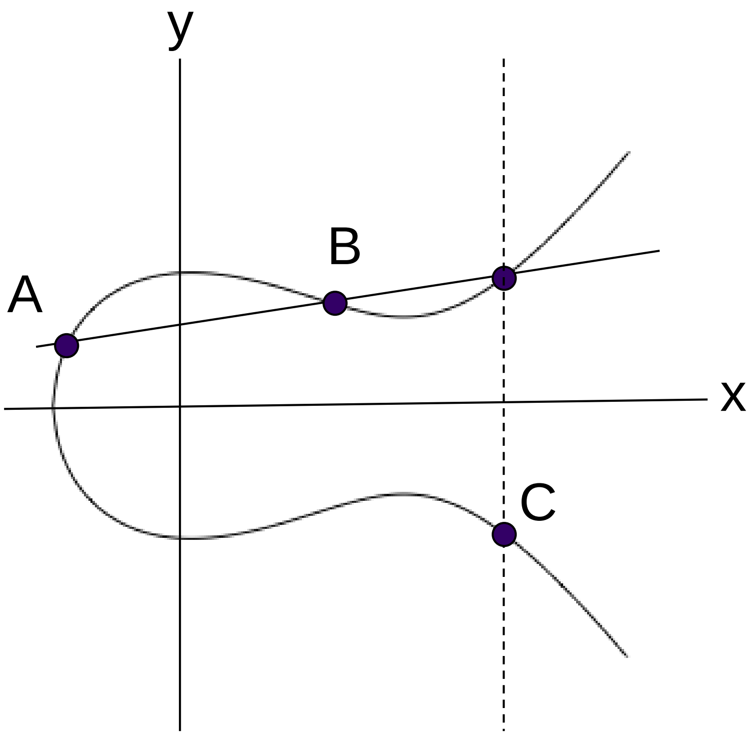


$$y^2 = x^3 - 3x + 3$$



$$y^2 = x^3 \ - 6x + 5$$

Review: EC operation: $\oplus$



$$C = A \oplus B$$

Review: Addition rules

- $P \oplus \mathcal{O} = P$
- $(x, y) \oplus (x, -y) = \mathcal{O}$
- $$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P = Q \end{cases}$$
- $P \oplus Q = (x_3, y_3)$
- $x_3 = (\lambda^2 - x_1 - x_2)$ & $y_3 = \lambda(x_1 - x_3) - y_1$

Review: Scalar multiplication

- $0P = \mathcal{O}$
- $1P = P$
- $2P = P \oplus P$
- $3P = P \oplus P \oplus P$
- $4P = P \oplus P \oplus P \oplus P$
- …

Elliptic curves mod p

- We take our elliptic curves mod p
  - p is prime

- Example $y^2 = x^3 + 3x + 8 \bmod 13$

$$\sqrt{1} = \{1,12\}, \sqrt{3} = \{4,9\}, \sqrt{4} = \{2,11\},$$
$$\sqrt{9} = \{3,10\}, \sqrt{10} = \{6,7\}, \sqrt{12} = \{5,8\}$$

- Points on curve

$$\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)$$

Adding two points

- Everything is mod 13
- $y^2 = x^3 + 3x + 8 \bmod 13$
- $P = (9,7) \quad Q = (1,8) \quad P \oplus Q = ?$
- $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-7}{1-9} = \frac{1}{-8} = \frac{1}{5} = 1 \cdot 5^{-1} = 8$
- $x_3 = \lambda^2 - x_1 - x_2 = 64 - 9 - 1 = 54 = 2$
- $y_3 = \lambda(x_1 - x_3) - y_1 = 8(9-2) - 7 = 49 = 10$
- $P \oplus Q = (9,7) \oplus (1,8) = (2,10)$

Adding two points

- Everything is mod 13
- $y^2 = x^3 + 3x + 8 \text{ mod } 13$
- $P = (9{,}7) \quad 2P = P \oplus P = ?$
- $\lambda = \frac{3x^2 + A}{2y} = \frac{3 \cdot 9^2 + 3}{2 \cdot 7} = \frac{246}{14} = \frac{12}{1} = 12$
- $x_3 = \lambda^2 - x_1 - x_2 = 144 - 9 - 9 = 126 = 9$
- $y_3 = \lambda(x_1 - x_3) - y_1 = 12(9 - 9) - 7 = -7 = 6$
- $2P = P \oplus P = (9{,}7) \oplus (9{,}7) = (9{,}6)$

Addition table

- $y^2 = x^3 + 3x + 8 \bmod 13$

	$\mathcal{O}$	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
$\mathcal{O}$	$\mathcal{O}$	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
(1,5)	(1,5)	(2,10)	$\mathcal{O}$	(1,8)	(9,7)	(2,3)	(12,2)	(12,11)	(9,6)
(1,8)	(1,8)	$\mathcal{O}$	(2,3)	(9,6)	(1,5)	(12,11)	(2,10)	(9,7)	(12,2)
(2,3)	(2,3)	(1,8)	(9,6)	(12,11)	$\mathcal{O}$	(12,2)	(1,5)	(2,10)	(9,7)
(2,10)	(2,10)	(9,7)	(1,5)	$\mathcal{O}$	(12,2)	(1,8)	(12,11)	(9,6)	(2,3)
(9,6)	(9,6)	(2,3)	(12,11)	(12,2)	(1,8)	(9,7)	$\mathcal{O}$	(1,5)	(2,10)
(9,7)	(9,7)	(12,2)	(2,10)	(1,5)	(12,11)	$\mathcal{O}$	(9,6)	(2,3)	(1,8)
(12,2)	(12,2)	(12,11)	(9,7)	(2,10)	(9,6)	(1,5)	(2,3)	(1,8)	$\mathcal{O}$
(12,11)	(12,11)	(9,6)	(12,2)	(9,7)	(2,3)	(2,10)	(1,8)	$\mathcal{O}$	(1,5)

How many points in an EC mod p?

- $y^2 = x^3 + Ax + B \mod p$
- Needs to be a square (true about 50% of time)
- Has two square roots (unless it is zero – rare)
- p possible values of x
- $\mathcal{O}$ is also a point

- Number of points about

$$50\% \cdot 2 \cdot p + 1 = p + 1$$

Hasse's theorem

- # of points in an elliptic curve mod $p =$
$$p + 1 - t_p$$
where t_p satisfies $|t_p| \leq 2\sqrt{p}$
- t_p is called "trace of Frobenius"
- Consider E: $y^2 = x^3 + 4x + 6 \bmod p$

p	$\#E$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	-2	4.47
7	11	-3	5.29
11	16	-4	6.63
13	14	0	7.21
17	15	3	8.25

Discrete logarithm problem

- Fix a prime p and a generator $g \in \mathbb{Z}_p$
- Discrete logarithm problem:

Given $a \in \mathbb{Z}_p$, find k such that $g^k \equiv a \pmod{p}$

- Fix an elliptic curve E mod p and a point P
- Discrete logarithm problem:

Given $Q \in E$, find k such that $kP = Q$

Best algorithms for discrete log

- Discrete log mod p

$$e^{((c+o(1))(\log p)^{1/3}(\log\log p)^{2/3})}$$

- Discrete log over elliptic curve mod p

$$\sqrt{p}$$

- Elliptic curves make things <u>much</u> harder

Diffie-Hellman key exchange

Alice

Bob

prime p, generator $g \in \mathbb{Z}_p$ $\longrightarrow$

$g^A \bmod p$ $\longrightarrow$

$\longleftarrow$ $g^B \bmod p$

$(g^B)^A \mod p$

$(g^A)^B \mod p$

Diffie-Hellman key exchange

Alice

Bob

Elliptic Curve $E \bmod p, P \in E$ $\longrightarrow$

$n_A P$ $\longrightarrow$

$n_B P$ $\longleftarrow$

$n_A(n_B P)$

$n_B(n_A P)$

Elgamal cryptosystem

- Referee
  - prime p, generator g
- Bob
  - random $x \in \{1, 2, \ldots, (p-2)\}$
  - $y = g^x \pmod{p}$
  - public key (p, g, y); secret key x
- Alice
  - message M, random $k \in \{1, 2, \ldots, (p-2)\}$
  - $a = g^k; b = My^k \pmod{p}$
  - transmits $\langle a, b \rangle$
- Bob
  - $b(a^x)^{-1} = My^k (g^{kx})^{-1} = M(g^x)^k g^{-xk} = M \pmod{p}$

Elgamal cryptosystem

- Referee
  - elliptic curve $E \bmod p, P \in E$
- Bob
  - Picks random x
  - $Q = xP$
  - public key (E, P, Q); secret key x
- Alice
  - message $M \in E$, random k
  - $A = kP; B = M \oplus kQ$
  - transmits $\langle A, B \rangle$
- Bob
  - $B \oplus (-x)A = M \oplus kQ \oplus (-x)kP = M \oplus xkP \oplus (-x)kP = M$

Next lecture

- Psuedo-random number generation
- SSL