CIS 3362 11/9/26

(1) Congrats UCF Prog Team

(2) Review Cyclic Nature of points on an Elliptic Curve

(3) How to encrypt a point using El Gamel

(4) How to exchange a key using Diffie-Hellman

(5) How to convert a bitstring to a point on an Elliptic Curve

(6) Don't go looking for prizes!

Origin satisfies

$P + O = P$, $O + O = O$, $O + P = P$

Additive Identity

So, if $kP = O$, then $(k+x)P = xP$.

List $P, 2P, 3P, \ldots$ is cyclic wrapsaround just like modular exponentiation (mod a prime)

Period of $(3,10)$ on $E_{23}(1,1)$ is 28.

A difficult problem w/ Elliptic Curves is:

Given kP, $k \in \mathbb{Z}$, P is a point on an Elliptic Curve $E_p(a,b)$, and given P, what is k?

$P=(3,10)$ $kP = (6,19)$ on $E_{23}(1,1)$

What is k?

Given P and k we <u>can</u> compute kP quickly

```
multiply (P, k):
    if k==1
        return P
    if k%2 == 0:
        ans = multiply(P, k/2)
        return add(ans, ans)
    return add(P, multiply(P, k-1))
```

runtime is $\log(k)$

Diffie-Hellman Key Exchange via Elliptic Curves:

Public key: $E_p(a,b)$ Pick a curve

$G = (x_1, y_1)$ $G \in E_p(a,b)$

and its order is large!

Alice picks private key n_A sends Bob

$n_A \times G$

Bob picks private key n_B sends Bob

$n_B \times G$ Eve sees this

Alice receives $(n_B \times G)$ she computes

$n_A \times (n_B \times G) = (n_A \times n_B) \times G$ ✓

Bob receives $(n_A \times G)$ he computes

$n_B \times (n_A \times G) = (n_A \times n_B) \times G$ ✓

Eve is unable to determine n_A or n_B.

Reg diffie hellman

Alice $g^a \rightarrow$ Bob $(g^a)^b = g^{ab}$

Bob $g^b \rightarrow$ Alice $(g^b)^a = g^{ab}$

El-Gamal Cryptosystem via Elliptic Curves

Alice sets up:

Public key $E_p(a,b)$ Curve

$G \in E_p$ Point w/large order

Private key Alice: $n_A < n$, n = order

Alice Public key = P_A $= n_A \times G$.

Let's say Bob wants to send a message, P_m, a point on curve. Bob picks $k < n$, k is secret.

Computes $C_1 = kG$ $C_2 = P_m + kP_A$

Alice receives (C_1, C_2)

1. She computes $n_A C_1 = (n_A \times k)G$
2. She computes $C_2 - n_A C_1$

$$= P_m + kP_A - n_A C_1$$
$$= P_m + k \cdot n_A G - (n_A \times k)G$$
$$= P_m$$

How do we take an arbitrary bit string and convert it to a point on an elliptic curve?

Idea #1: make the message = x

take $y^2 = x^3 + ax + b \pmod p$

plug in x. Solve for y.

Issue #1: Some values of ~~y~~ x produce ~~and~~ an equation with NO sol for y.

Issue #2: If there is a solution for y, how do we find it?

It turns out that roughly $\frac{1}{2}$ of the x values have matching y's.

extra 16 bits | plaintext 512 bits = 528 bits let's prime p is 528 bits

00...0 Plaintext → Does this work? 50% ↓

00...1 Plaintext → Does this work? 50% ↓

⋮

2^{16} possible strings I can pre-pend prob failure every time is $\left(\frac{1}{2}\right)^{2^{16}} = \left(\frac{1}{2}\right)^{65536}$

Given $y^2 = x^3 + ax + b \pmod{p}$

1) Compute for a given x $\quad c = x^3 + ax + b \pmod{p}$

2) Does $y^2 \equiv c \pmod{p}$ have a solution?

Quadratic Residue Problem

Legendre Symbol:

$\left(\frac{c}{p}\right) \equiv 1$ if $y^2 \equiv c \pmod{p}$ has a solution and $c \neq 0$

$\left(\frac{c}{p}\right) \equiv -1$ if $y^2 \equiv c \pmod{p}$ has no solution

$\left(\frac{c}{p}\right) \equiv 0$ if $c = 0$.

Euler figured out that $c^{\frac{p-1}{2}}$

$$\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \pmod{p}$$

if $\left(\frac{c}{p}\right) \equiv c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

then how do I find y?

$$y \equiv c^{\frac{p+1}{4}} \pmod{p}$$

$$y^2 \equiv \left(c^{\frac{p+1}{4}}\right)^2 \equiv c^{\frac{p+1}{2}} \equiv \boxed{c^{\frac{p-1}{2}}} \times c^1 \quad \left[\frac{p+1}{2} = \frac{p-1}{2} + \frac{2}{2} = \frac{p-1}{2} + 1\right]$$

$$\equiv 1 \times c$$

$$\equiv c \pmod{p}$$

$$c \times c^{\frac{p-1}{2}} \equiv c \times 1 \pmod{p}$$

$$c^{\frac{p+1}{2}} \equiv 1 \pmod{p}$$

if $y^2 \equiv c^{\frac{p+1}{2}}$, then $y \equiv c^{\frac{p+1}{4}} \bmod p$

What has to be true for $\frac{p+1}{4}$ to exist as an exponent in this context?

$$\frac{p+1}{4} = n \qquad p+1 = 4n \qquad p = 4n-1,\ n \in \mathbb{Z}$$

$$p = 4n'+3,\ n' \in \mathbb{Z}$$

In order for this to work you must pick a prime $p \equiv 3 \pmod 4$.