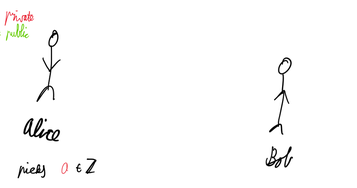
Lecture 2

Thursday, 8 September 2022 10:46

Diffie - Hellman key exchange

- Everybody knows $P = (x, y)$ and how to compute $P + P = 2P$, $3P = 2P + P$, $kP = \underbrace{P + P + \dots + P}_{k \text{ copies of } P}$

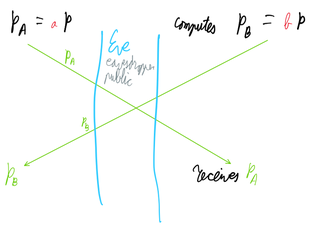
red = private
green = public



Alice picks $a \in \mathbb{Z}$

Bob picks $b \in \mathbb{Z}$

Alice computes $P_A = aP$ | Bob computes $P_B = bP$



Alice computes $aP_B = a(bP) = b(aP) = bP_A$ Bob computes

Alice & Bob now share $(ab)P$, e.g. a hash function
the they use a key-derivation function to derive a shared key in $\{0,1\}^n$ (strings of length n) to use symmetric cryptography

Computational DH problem (CDHP)
given P, P_A, P_B compute $(ab)P$

easy if solved

decisional DH problem (DDHP)
given P, P_A, P_B and Q, decide whether $Q = abP$

trivial if solved

discrete logarithm problem (DLP)
given P, P_A, compute a

in other words:

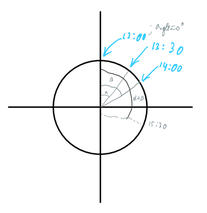
solving DLP means solving CDHP

solving CDHP means solving DDHP

the other way around: only for some groups DLP & CDHP

groups in which DDHP is easy and CDHP is not are called gap groups

What is P?
and $P + P$?



Any point satisfies
$x^2 + y^2 = 1$
$12{:}00 \doteq (0, 1)$
$13{:}30 \doteq \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) = \left(\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{2}\right)$
$14{:}00 \doteq \left(\frac{1}{2}\sqrt{3}, \frac{1}{2}\right)$

We add points at angles α and β to get the point at $\alpha + \beta$.
(Could also speak about adding radii or areas)

What time is $\left(\frac{3}{5}, \frac{4}{5}\right)$? $2\left(\frac{3}{5}, \frac{4}{5}\right)$

Get rid of α, β; we want to use x, y

Note that we are defining angle = 0 differently from physics

$$(x_1, y_1) + (x_2, y_2) = (\sin\alpha_1, \cos\alpha_1) + (\sin\alpha_2, \cos\alpha_2) = (\sin(\alpha_1 + \alpha_2), \cos(\alpha_1 + \alpha_2))$$
$$= (\sin\alpha_1 \cos\alpha_2 + \cos\alpha_1 \sin\alpha_2, \cos\alpha_1 \cos\alpha_2 - \sin\alpha_1 \sin\alpha_2)$$
$$= (x_1 y_2 + y_1 x_2, y_1 y_2 - x_1 x_2)$$

$$\left(\frac{3}{5}, \frac{4}{5}\right) + \left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{24}{25}, \frac{7}{25}\right)$$

$$3\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{117}{125}, -\frac{44}{125}\right)$$
$$4\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{336}{625}, -\frac{527}{625}\right)$$
$$a\left(\frac{3}{5}, \frac{4}{5}\right) = \left(\frac{?}{5^a}, \frac{?}{5^a}\right)$$

so the size of the denominator gives away a :(
Eve just computes the log bases.

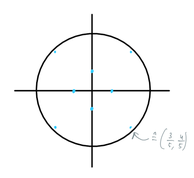
Exc: Compute modulo a prime, e.g. $p = 1{,}000{,}003$

$p = (1000, 2)$ is on the circle mod 1000003 (as $1000^2 + 2^2 = 1000004 \equiv 1 \bmod 1000003$)

Clock mod 7: $x^2 + y^2 \equiv 1 \bmod 7$
$(0, \pm 1), (\pm 1, 0), (\pm 2, \pm 2)$ signs take independently

does $x = 3$ give a point
$3^2 + y^2 \equiv 2 + y^2 \equiv 1 \bmod 7$
requires $y^2 \equiv -1 \bmod 7$, but 2 is congruent to 3 mod 4 and thus -1 is not a square modulo 7
Hence there is no point with $x = \pm 3$

All points are $\{(0, \pm 1), (\pm 1, 0), (\pm 2, \pm 2)\}$



8 points on clock mod 7

$3 \cdot 5 = 15 \equiv 1 \bmod 7$
$2 \cdot \frac{1}{2} \equiv 1$

previous example $\left(\frac{3}{5}, \frac{4}{5}\right) \doteq (3 \cdot 3, 4 \cdot 3)$ $\equiv 4 \bmod 7$
$= (2, 5) = (2, -2)$

Back to $p = 1000003$
$P = (1000, 2)$
$2P = (4000, 4 - 1000000)$
$\equiv (4000, 4 + 3) \bmod p$
$\equiv (4000, 7) \bmod p$

If I multiply I still see the sizes grow but soon reduction mod p hides it.

HW: find a for a big point
Homework
use sagemath.org to solve
or Python, or...

Clocks mod p are part of secure

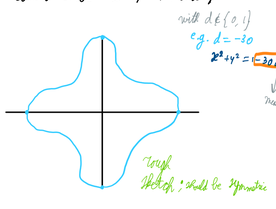
Normally want: exponential growth in attack cost, i.e. working with n bits should cause attack cost of $O(2^{\frac{n}{6}})$ for small ϵ

Really bad: polynomial time attacks, e.g. perfect code system

Clocks mod p have attacks that run in sub-exponential but superpolynomial time

$$e^{c \log^{\frac{1}{3}} p \log\log^{\frac{1}{3}} p}$$

Edwards curve $x^2 + y^2 = 1 + d x^2 y^2$
with $d \in \{0, 1\}$
e.g. $d = -30$
$x^2 + y^2 = \boxed{1 - 30 x^2 y^2}$
Now working over modulo the prime



Exc over $\mathbb{R}$: our addition law has no "nice" interpretation (angles, radii, areas), but is very similar to circle addition law:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}\right)$$

numerators match the circle formulas

Edwards curves are due to Harold Edwards (2007), based on Gauss & Euler.