SECURITY (COMP0141):

MATH MEETS CRYPTOGRAPHY

UCL

MATH MEETS CRYPTOGRAPHY

Two interesting settings to consider from a cryptographic perspective:

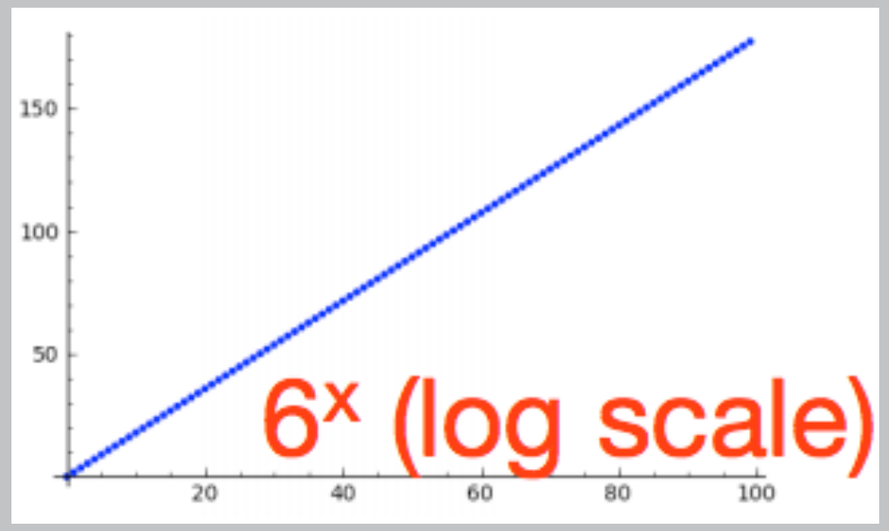
The finite field F_p for a very large prime p (1024 bits or more)

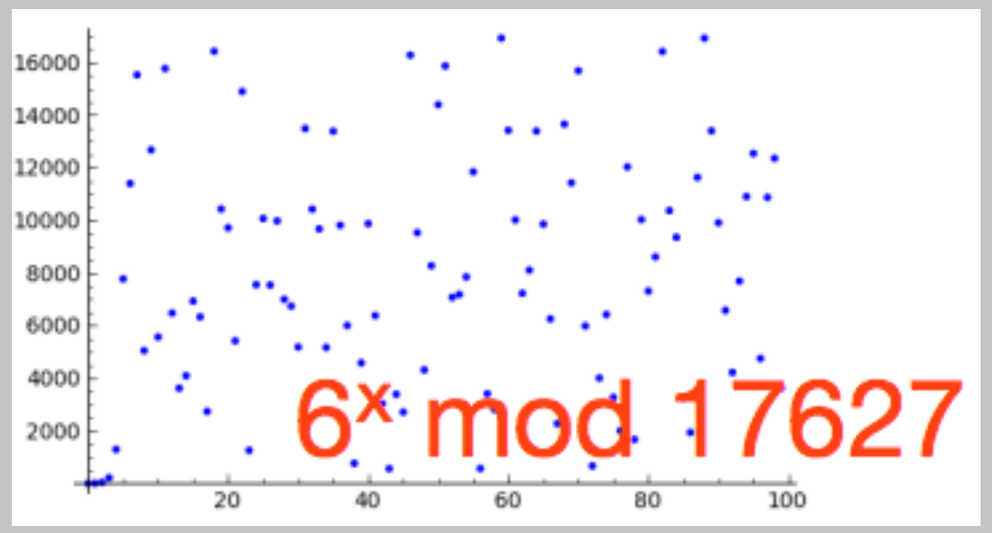
The ring (Z/NZ)* for N = pq for very large primes p,q (1024 bits or more)

DISCRETE LOGARITHM

Discrete logarithm problem: for a fixed prime p, given g and y, find x such that $g^x = y \bmod p$

Example: $6^x = 10000 \bmod 17627$





This problem seems to be very difficult to solve (like for modern computers and large enough p, until the heat death of the sun)

MATH MEETS CRYPTOGRAPHY

Two interesting settings to consider from a cryptographic perspective:

The finite field F_p for a very large prime p (1024 bits or more)

The ring (Z/NZ)* for N = pq for very large primes p,q (1024 bits or more)

THE RING (Z/NZ)*

Euler totient function φ is $\varphi(N) = \left|\{x \text{ in } \{0,\ldots,N-1\} \mid \gcd(x,N) = 1\}\right|$

Euler's theorem: $x^{\varphi(N)} = 1 \bmod N$ for $x \in (Z/NZ)^*$

Now let N = pq for p and q two different odd primes

RSA

RSA problem: given an integer N = pq, find p and q

Example: the RSA-1024 challenge is to find p and q for N =
135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879413773285339061097505443349998111500569772368909275636

THE RING (Z/NZ)*

Euler totient function φ is $\varphi(N) = \left|\{x \text{ in } \{0,\ldots,N-1\} \mid \gcd(x,N) = 1\}\right|$

Euler's theorem: $x^{\varphi(N)} = 1 \bmod N$ for $x \in (Z/NZ)^*$

Now let N = pq for p and q two different odd primes

$$\begin{aligned}\varphi(N) = \varphi(pq) &= pq - \left|x : \gcd(x,pq) \neq 1\}\right| \\ &= pq - \left|\{x : p \mid x\}\right| - \left|\{x : q \mid x\}\right| + \left|\{0\}\right| \\ &= pq - q - p + 1 = (p-1)(q-1)\end{aligned}$$

This means that $(Z/NZ)^*$ has $\varphi(N) = (p-1)(q-1)$ elements

ONE-WAY FUNCTIONS

More generally, discrete log and RSA are examples of something called a **one-way function**

This is a function f( ) such that

-(1) it is easy to compute f(x) for all x, but

-(2) it is assumed to be very difficult to compute x given f(x), or in fact to compute any y such that f(y) = f(x)

Discrete log: $f(x) = g^x \bmod p$

RSA: f(p,q) = pq