Recall Diffie-Hellman Key Exchange

Trusted publishes p and $g \in \mathbb{F}_p^*$ of large prime order

- **Alice** picks secret $a \in \mathbb{Z}$, sends $A \equiv g^a \mod p$ to Bob
  Bob picks secret $b \in \mathbb{Z}$, sends $B \equiv g^b \mod p$ to Alice

- **Alice** computes $A' \equiv B^a \mod p$
  Bob computes $B' \equiv A^b \mod p$

- Shared key is $A' = B'$

Diffie-Hellman parameters in `https://www.ietf.org/rfc/rfc3526.txt`

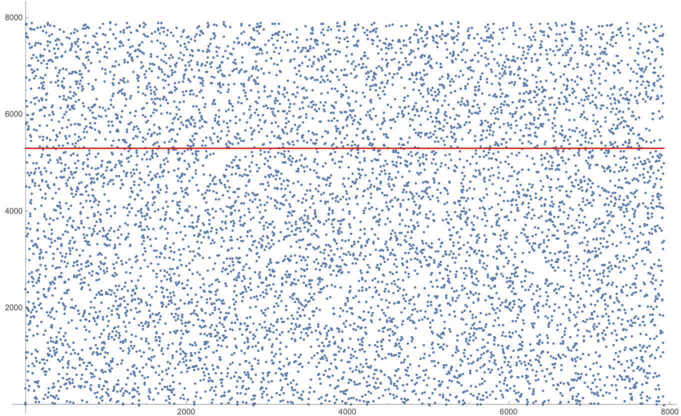
The 8192-bit mod p group uses

$$p = 2^{8192} - 2^{8128} - 1 + 2^{64} \cdot (\lfloor 2^{8062} \cdot \pi \rfloor + 4743158)$$

Why is the DLP $g^x \equiv h \mod p$ hard?

If g has large order, then exponentiation mod p mixes really well

Solve $7^x \equiv 5314 \mod 7919$



Defintion of a group

A **group** consists of a set G and a rule $\star$, for combining two elements $a, b \in G$ to obtain $a \star b \in G$. In addition, $\star$ must have the following three properties:

- **Identity Law:** There exists $e \in G$ such that $e \star a = a \star e = a$ for all $a \in G$
- **Inverse Law:** For every $a \in G$, there exists $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$
- **Associative Law:** $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in G$

1. (a) Fill in the addition table for $\mathbb{Z}/4\mathbb{Z}$, then relabel $\{0, 1, 2, 3\} \to \{e, a, b, c\}$ and rebuild the table

+	0	1	2	3
0				
1				
2				
3				

+	e	a	b	c
e				
a				
b				
c				

(b) Fill in the multiplication table for $\mathbb{F}_5^*$, then relabel $\{1, 2, 3, 4\} \to \{e, a, c, b\}$ and rebuild the table

×	1	2	3	4
1				
2				
3				
4				

×	e	a	b	c
e				
a				
b				
c				

(c) What do you notice about your relabeled tables?

2. For each group G and element $a \in G$, compute the order of G and the order of a. Verify that $\text{ord}(a) \mid |G|$
   (a) $G = \mathbb{Z}/12\mathbb{Z}$, $a = 7$

   (b) $G = \mathbb{Z}/12\mathbb{Z}$, $a = 8$

   (c) $G = (\mathbb{Z}/12\mathbb{Z})^*$, $a = 7$

   (d) $G = \mathbb{F}_{13}$, $a = 3$

   (e) $G = \mathbb{F}_{13}^*$, $a = 3$