

## ElGamal: ElGamal over Matrices

In “simple” ElGamal, operations are performed in the group  $\mathbb{Z}_p^*$ : If  $g$  is a primitive root of this group, then we compute  $h = g^\alpha \pmod{p}$ . Here,  $g$  is a public parameter,  $h$  is the public key, and  $\alpha \in \mathbb{Z}_{p-1}$  is a (random) private key.

We thought: Cool! Maybe we can create a more secure cryptosystem by computing over matrices: Let  $G$  be a  $5 \times 5$  matrix with entries over  $\mathbb{Z}_p^*$ . Define  $H = G^\alpha$ . As above,  $G$  is a public parameter,  $H$  is the public key, and  $\alpha \in \mathbb{Z}_{p-1}$  is a (random) private key.

Alas, some hacker totally broke our system, and found the private key  $\alpha$ . Can you do the same?!

The value  $p$ , as well as matrices  $G$  and  $H$  are defined in file `Matrices.txt`. Once you found  $\alpha$ , give it to `flag-gen.py` to compute the flag.