RSA

- **Alice – Key Creation**
  - Choose secret primes p and q, form $N = pq$
  - Choose exponent e with $\gcd(e, \phi(N)) = 1$
  - Compute private $d \equiv e^{-1} \mod \phi(N)$ using EEA
  - Publish (N, e)
- **Bob – Encrypt plaintext** $m \in \mathbb{Z}_N$
  - Use Alice's public key (N, e) to compute $c \equiv m^e \mod N$
  - Send ciphertext c to Alice
- **Alice – Decrypt ciphertext** c

$$c^d \equiv m^{de} \mod N \equiv m \mod N$$