Discussion 4

February 22, 2019

1 RSA

- Public key: (N, e) where $N = pq$ and e is relatively prime to $(p-1)(q-1)$.
- Private key: $d \equiv e^{-1} \mod (p-1)(q-1)$.
- Encoder function: $y = E_d(x) = x^d \mod n$. y is public.
- Decoder function: $D_e(y) = x^e \mod n$. With private key e, $x = D_e(y)$ recovers the original secret.