RSA:

Bob chooses
- large random primes p, q $\quad N := pq$
- e, d so that $ed \equiv 1 \pmod{\phi(N)}$

public key: $N = pq, e$	private key: d

Alice encrypts: $c = m^e \pmod N$
Bob decrypts: $m = c^d \pmod N$

COMMENTS:
- e doesn't have to be random; but must be invertible mod $\phi(N)$

EG If $N = 77$, what is smallest possible e?

$\phi(77) = \phi(7)\phi(11) = 6 \cdot 10 = 60$

$e = 1$ no encryption
$e = 2, 3, 4, 5, 6$ not invertible

$\Rightarrow e = 7$

- Decryption can be sped up using CRT
- $\phi(N) = (p-1)(q-1)$ can be replaced with $\operatorname{lcm}(p-1, q-1)$

  ⇝ key space a bit smaller
- RSA very slow compared to AES

  ⇝ used to establish shared secret; then use AES
- $m = 1$ always encrypted to $c = 1$, $m = 0$ always encrypted to $c = 0$ problem?

DO NOT ENCRYPT messages from a predictable set using deterministic public key cryptosystems

Fix: augment m with random noise

not an issue for AES