Crib 7

written by Alvin Wan . alvinwan.com/cs70

Monday, September 26, 2016

The crib sheet contains cheat-sheet worthy information but is not a substitute for lectures or for reading the notes. It also contains pointers and common mistakes.

1 RSA

- Our public key is (e, N), and our private key is d.
- We define our encryption function to be $E(x) = x^e = m$ and our decryption function to be $D(m) = m^d$, where x is the original message and m is the encrypted message.
- Using these, we see that for $D(m) = x$ to be true, $ed = 1 (\text{mod } (p-1)(q-1))$.
- If N can be factored into p and q easily, RSA is broken (we can solve for the multiplicative inverse of e in mod (p-1)(q-1).