COMP 2711 Tutorial

Week 11

YEUNG, Chun Kit
Computer Science and Engineering
Hong Kong University of Science and Technology
email: ckyeungac@connect.ust.hk

November 14, 2017

Who is this guys?

- New TA responsible for the rest of semester
- Graduated from HKUST (ask me anything if you have other questions as well)
- Speak English, Mandarin, and native in Cantonese.
- Machine learning in education is what I am doing now.
- It has been 4 years ago when I took COMP 2711 in my UG.

Common Divisor

- $m|n$ means m divides n, e.g. $5|30$.
- If b be the common divisor of (m_1, m_2), then we could express $b = k_1 m_1 + k_2 m_2$, for some integer k_1 and k_2.
- Why? Let's say

$$m_1 = b \cdot n_1$$
$$m_2 = b \cdot n_2$$

Then, if $k_1 n_1 + k_2 n_2 = 1$, the following equation is established

$$\begin{aligned} b = b \cdot 1 &= b(k_1 n_1 + k_2 n_2) \\ &= k_1 b n_1 + k_2 b n_2 \\ &= k_1 m_1 + k_2 m_2 \end{aligned}$$

RSA

1. Select a large prime p and q, such that $n = pq$.
2. Select a encryption key e with $gcd(\phi(n), e) = 1$, where $1 \leq e \leq \phi(n)$ and $\phi(n) = (q-1)(p-1)$.
3. Compute the decryption key d: d is the multiplicative inverse of e, i.e.

$$de \bmod \phi(n) = 1$$

4. Encryption process: $C = M^e mod n$.
5. Decryption process: $M = C^d mod n$.

There is a nice video explaining public key cryptography using an analog of color mixing: Public key cryptography: What is it? [2:55]