Alison Li

RSA Protocol

(1) Ann sets $n = pq$ (p, q large primes).
Let k be public key, s be private key. Find k, s such that $ks \equiv 1 \pmod{(p-1)(q-1)}$.
Publish n, k.
(2) To encrypt m, compute $\bar{m} \equiv m^k \pmod{n}$.
(3) To decrypt, compute $\bar{m}^s \pmod{n} = m$.

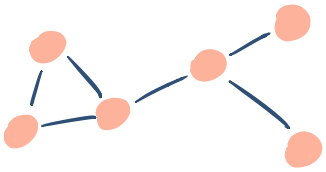
ex. With $p = 3$, $q = 11$, $n = 33$.
$(p-1)(q-1) = 2 \cdot 10 = 20$.
Choose $k = 7$, $s = 3$ (since $7 \cdot 3 \equiv 21 \equiv 1 \pmod{20}$).
To send message m, m in range $0, 1, \ldots, 32$.
In terms of bits, can use up to 5 bits since $2^5 = 32$.
Want to send $m = 00010$.
$10 = m = 2$. Encrypt as $\bar{m} = m^k = 2^7 \equiv 128 \pmod{33}$
$\equiv 99 + 29 \equiv 29$.
Send $\bar{m} = 29$.
Decrypt $\bar{m}^s = 29^3 \equiv (-4)^3 \equiv (-64) \equiv 2 = m$.

Note: If "29" is intercepted, trying to recover $m = 2$ by $29^{1/7} = 1 \cdot 61$ is not helpful. No obvious way to get the message.

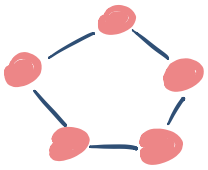
Why does $\bar{m}^s \equiv m \pmod{n}$?
Lemma.
If $a \equiv b \pmod{k\ell}$ then $a \equiv b \pmod{k}$ and $\pmod{\ell}$.
proof (lemma ↑).
$a \equiv b \pmod{k\ell} \Rightarrow k\ell \mid b-a \Rightarrow b-a = k\ell r$ some $r \in \mathbb{Z}$
so $k \mid b-a$ so $a \equiv b \pmod{k}$. Similar for ℓ. □
proof ($\bar{m} \equiv m \pmod{n}$).
We know $ks \equiv 1 \pmod{(p-1)(q-1)}$.
So $\ell(p-1)(q-1) = 1 - ks$.
$ks = 1 - \ell(p-1)(q-1)$.
Since k, s both positive, $\ell < 0$ i.e. $-\ell > 0$.
Consider $\bar{m}^s \equiv (m^k)^s \equiv m^{ks} \pmod{n}$ (Note: $n = pq$)
$\equiv m^{1-\ell(p-1)(q-1)}$
By lemma, $\bar{m}^s \equiv m^{1-\ell(p-1)(q-1)} \pmod{p}$
$\equiv m(m^{(p-1)})^{-\ell(q-1)} \pmod{p}$ (Note: $-\ell(q-1)$ positive)
$\equiv m(1)^{-\ell(q-1)} \pmod{p}$ by Fermat, unless $m \equiv 0 \pmod{p}$
$\equiv m \pmod{p}$.
Similarly for q, $\bar{m}^s \equiv m \pmod{q}$ (unless $m \equiv 0 \pmod{q}$).
So,
$p \mid \bar{m}^s - m$, $q \mid \bar{m}^s - m$.
Since $\gcd(p, q) = 1$ (assume $p \neq q$).
$pq \mid \bar{m}^s - m$ (lemma)
So $\bar{m}^s \equiv m \pmod{n}$.
One missing case: If $m \equiv 0 \pmod{p}$ or $m \equiv 0 \pmod{q}$.
(It works, omit proof.) □

Security of RSA.
Suppose $\bar{m}$ is intercepted. n, k are known.
(1) If $m^k < n$, then $(\bar{m})^{1/k} = (m^k)^{1/k} = m$.
(no mod here; integers!) Don't send if $m^k < n$.
(2) If you can factor $n = pq$, you can find $[k]^{-1} = [s]$ in $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$,
i.e. find s, then use it to decrypt.
So, security is based on difficulty of factoring integers.
This is, so far, a difficult problem.

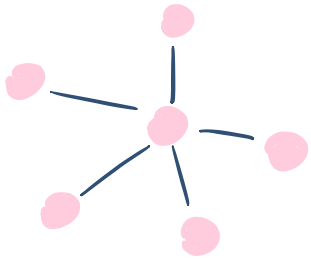
Graph Theory



Graph has vertices connected by edges.
Only important info is which vertices are connected.



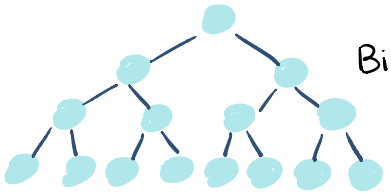
Circle graph C_n
This is C_5.



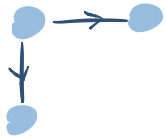
Star graph

line / Path graph

Important but not focus:

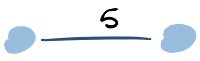


Binary tree



Directed graph

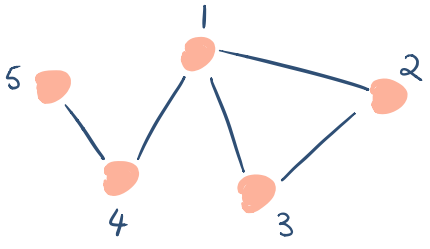
multi-edges



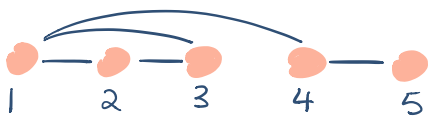
Weighted edges

def. A finite simple graph ("graph") is a pair $G = (V, E)$ where V is a finite set (vertices) and $E \subseteq \{\{v_1, v_2\} \mid v_1, v_2 \in V \; v_1 \neq v_2\}$ (edges).

ex. $G = (V, E)$ with $V = \{1, 2, 3, 4, 5\}$, $E = \{\{1,2\}, \{1,4\}, \{4,5\}, \{2,3\}, \{1,3\}\}$.
It can be drawn as:



or



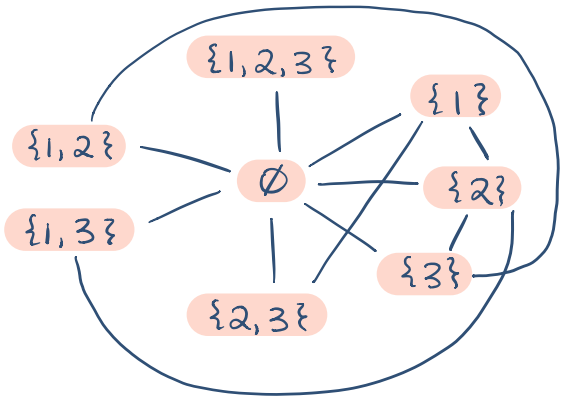
Orientation in space is not relevant.
Drawing is just a visualization.

Quson Li

Notation: For simplicity, write (v_1, v_2) rather than $\{v_1, v_2\}$.

def. If $e = (v_1, v_2)$ is an edge, its end points are v_1, v_2 and e is said to be incident on v_1, v_2.

ex. Let $G = (V, E)$ with $V = \mathcal{P}(\{1,2,3\})$ and $(A, B) \in E \Leftrightarrow A \cap B = \emptyset$.
Sketch G:

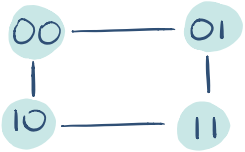


def. The n-dimensional hypercube or Hamming cube is a graph Q_n where $V = \{0,1\}^n$ = binary strings of length n.
$(s_1, s_2) \in E \Leftrightarrow s_1, s_2$ differ in exactly one bit

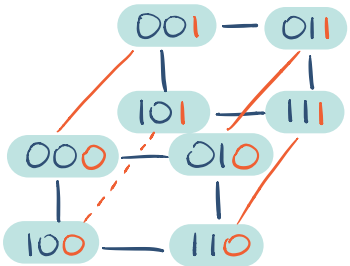
Sketch of Q_1, Q_2, Q_3, Q_4:

Q_1:

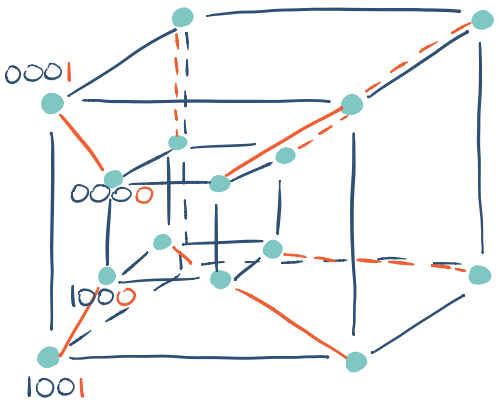
Q_2:



Q_3: Make two copies of Q_2.
Append '0' to vertices of copy, and '1' to the other.
Connect the corresponding vertices.



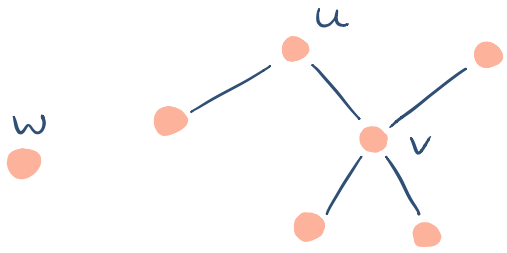
Q_4:



def. The degree of a vertex v is the number of edges incident (attached) to v. Denoted deg(v).

def. u, v are adjacent if $(u,v) \in E$.
The neighbours of v are u such that $(v,u) \in E$.

ex.

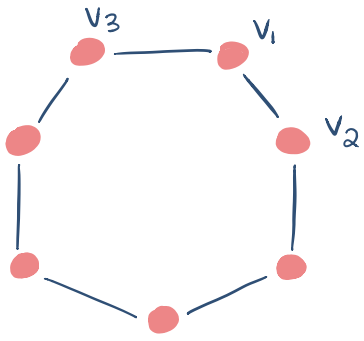


deg(v) = 4
deg(u) = 2
deg(w) = 0

v has 4 neighbours.

def. G is called k-regular if $\forall v \in V$, deg(v) = k.

ex.



C_n is 2-regular.
Neighbours of v_1 are v_2, v_3.

Q_n hypercube is n-regular. Each string has length n, so you can change any one of the bits. This gives the n neighbours. Hence, degree is n for all v.