The RSA encryption algorithm.

Say Bubba wants to send a message to Ashley.

1. Ashley picks p & q to be very large prime numbers, lets $n = pq$
   (easy to do)

2. Ashley computes $\varphi(n) = pq - q - p + 1$
   & picks a large number e relatively prime to n s.t.
   $$1 << e < \varphi(n).$$
   Ashley sends Bubba the "public key" $= (n, e)$. $(e \approx 2^{16}+1$

   easy

3. Bubba wants to send the message m (a number).
   Bubba computes $c = m^e \bmod n$ quick to do on computer.
   the encrypted message.
   Bubba sends c to Ashley.

4. Ashley computes $m = c^d \bmod n$.

   (d = multiplication inverse of e mod $\varphi(n)$ easy for Ashley to find.
   $de \equiv 1 \bmod \varphi(n)$)

   This gives Ashley the message.

How does this work?

$$c = m^e \mod n$$

$$c^d = m^{de} \mod n$$

$$de = 1 \mod \varphi(n)$$

$$\Rightarrow c^d = m^{1+k\varphi(n)} \mod n$$

$$= m^1 \cdot \big(\underbrace{m^{\varphi(n)}}_{\text{Euler's Thm } = 1}\big)^k \mod n$$

$$= m \mod n \,!$$

Why is this good?

Knowing $(n, e) \rightarrow$ very hard to find p & q.

$\rightarrow$ don't know d.

Example of inhomogeneous recursion.

Suppose $a_0 = 1$, $a_1 = -2$

$$a_{n+1} = 4a_n + 5a_{n-1} + 2(-1)^n - n$$

Solution: ① Homogeneous Solution:

$$a_{n+1} = 4a_n + 5a_{n-1}$$

Try $a_n = r^n \Rightarrow r^{n+1} = 4r^n + 5r^{n-1}$

$$\Rightarrow r^{n+1} - 4r^n - 5r^{n-1} = 0$$

factor out r^{n-1} $\Rightarrow r^2 - 4r - 5 = 0$

$$(r-5)(r+1) = 0$$

$$\Rightarrow r = 5 \text{ or } -1.$$

Gen Hom soln. $a_n = c_1 5^n + c_2 (-1)^n$.

② Particular Solution

. Extra $2(-1)^n - n$

Try:

$$a_n = K\underset{\uparrow}{n}(-1)^n + An + B$$

added n because $(-1)^n$ is hom. solution

Plug in: $a_{n+1} = 4a_n + 5a_{n-1} + 2(-1)^n - n$

$$K(n+1)(-1)^{n+1} + A(n+1) + B$$
$$= 4(Kn(-1)^n + An + B) +$$
$$5(K(n-1)(-1)^{n-1} + A(n-1) + B) + 2(-1)^n - n$$

$$(-1)^{n-1} = -(-1)^n$$

$$(-1)^{n+1} = -(-1)^n$$

$$(-1)^n\left[-Kn-K\right]+An+(A+B)$$

$$=(-1)^n\left[4Kn-5Kn+5K+2\right]$$

$$+n\left[4A+5A-1\right]+\left[4B-5A+5B\right]$$

equations

$n(-1)^n$: $-K=-K \Rightarrow$ nothing.

$(-1)^n$: $-K=5K+2 \Rightarrow -6K=2$, $K=\frac{-1}{3}$

n: $A=9A-1$ $\quad 1=8A \Rightarrow A=\frac{1}{8}$

1: $A+B=9B-5A$ $\quad 6A=8B$, $B=\frac{3}{4}A=\frac{3}{32}$.

Part. Solution is

$$a_n=Kn(-1)^n+An+B=\frac{-1}{3}n(-1)^n+\frac{1}{8}n+\frac{3}{32}$$

Gen Inhom Solution:

$$a_n = C_1 5^n + C_2(-1)^n - \frac{1}{3}n(-1)^n + \frac{1}{8}n + \frac{3}{32}$$

Plug in initial conditions $a_0 = 1$, $a_1 = -2$

$$a_0 = 1 = C_1 + C_2 + \frac{3}{32}$$

$$a_1 = -2 = 5C_1 - C_2 + \frac{1}{3} + \frac{1}{8} + \frac{3}{32}$$

solve for C_1, C_2

Plug in.