Feb 13-th

Reciever pick two distinct primes p, q

Computes $N = pq$

Computes $\varphi(N) = (p-1)(q-1)$

picks a number E (encoder)

Relatively prime $\varphi(N)$

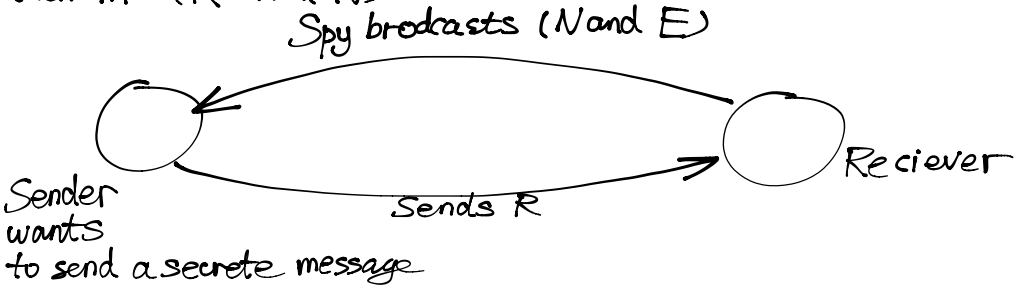
$\gcd(E, \varphi(N)) = 1$

Sender wants to sent a secrete message $1 \leq n < N$
Sender picks $R = M^E \pmod N$

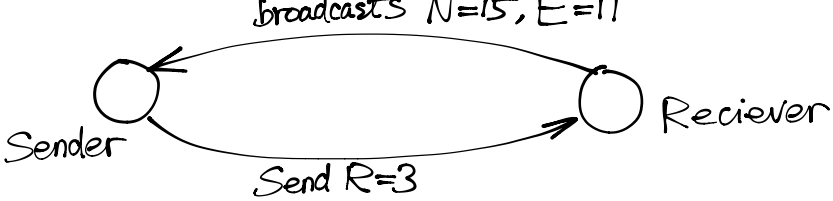
Reciever gets R, wants to recover M reciever.
find D. s.t.

$$DE \equiv 1 \bmod \varphi(N)$$

always possible since $\gcd(E, \varphi(N)) = 1$ D-decoder
then $M = (R^D \bmod N)$



$p=3, q=5, N=3\cdot 5=15$
$\varphi(N) = 2\cdot 4 = 8$ pick $E=11$, $\gcd(11, 8)=1$



Reciever gets $R=3$, wants to recover M.

We want D-decoder s.t.
$DE \equiv 1 \bmod \varphi(N)$
$D \cdot 11 \equiv 1 \bmod 8$

$\gcd(11, 8) = 1$ want $11D - 8K = 1$ D, K. integers, then $11D \equiv 1 \bmod 8$

We can do this using the Euclidean Algorithm

$11 = 1\cdot 8 + 3$
$8 = 2\cdot 3 + 2$
$3 = 1\cdot 2 + 1$
$2 = 2\cdot 1 + 0$
$1 = \gcd(11, 8)$

$3 = 11\cdot 1 - 8\cdot 1$
$2 = 8\cdot 1 - 3\cdot 2$
$= 8\cdot 1 - (11\cdot 1 - 8\cdot 1)\cdot 2$
$= 8\cdot 3 - 11\cdot 2$
$1 = 3\cdot 1 - 2\cdot 1 = \cdots = 11\cdot 1 - 8\cdot 1 - 8\cdot 3 + 11\cdot 2$
$= 11\cdot 3 - 8\cdot 4$

Can take $D = 3$ decoder

Can recover M or $M = R^D \bmod N$
$R = 3, D = 3, N = 15$
$M \equiv 3^3 \bmod 15 \equiv 27 \bmod 15 \equiv 12 \Rightarrow M = 12$

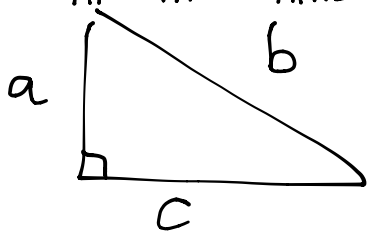
check : $R \equiv M^E \bmod N$
$M = 12, E = 11$
need to compute $12^{11} \bmod 15$

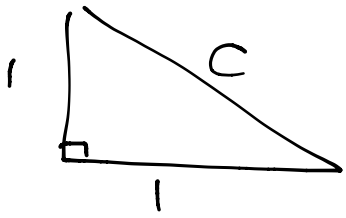
$12 \equiv -3 \bmod 15$
$12^3 \equiv (-3)^3 \equiv -27 \equiv 3 \bmod 15$
$12^9 \equiv (12^3)^3 \equiv 27 \equiv -3 \bmod 15$
$2^{11} \equiv 12^9 \cdot 12^2 \equiv (-3)(-3)^2 \equiv -27 \equiv 3 \bmod 15$
$\Rightarrow 2^{11} \equiv 3 \bmod 15$

Irrational Numbers
A number is called rational if it can be written as a function $\frac{m}{n}$ where m, n are integers

$a = \frac{m_1}{n_1}$, $b = \frac{m_2}{n_2}$ are rational $\Rightarrow a+b, a-b, ab, \frac{a}{b}$ are rational too.

$a \cdot b = \frac{m_1}{n_1} \cdot \frac{m_2}{n_1} = \frac{m_1 m_2}{n_1 n_2}$





$a^2 + b^2 = c^2$

$c^2 = 1^2 + 1^2$
$c^2 = 2 \Rightarrow c = \sqrt{2}$

claim : $\sqrt{2}$ is irrational (i.e. not rational)

Proof:
Suppose $\sqrt{2} = \frac{m}{n}$ for some m, n integers
If $\gcd(m, n) = d \neq 1 \Rightarrow$ we can write $m = dm$, $n = dn$
$\gcd(m, n) = 1$

$$\sqrt{2}=\frac{m}{n}=\frac{dm_1}{dm_2}=\frac{m_1}{n_1}$$

$$2=(\sqrt{2})^2=\left(\frac{m_1}{n_1}\right)^2 \Rightarrow 2=\frac{m_1^2}{n_1^2} \Rightarrow 2n_1^2=m_1^2$$

$\Rightarrow m_1^2$ is even $\Rightarrow m$ is even $\Rightarrow m_1=2m_2$

$m_1=2m_2 \Rightarrow$ both even
$n_1=2n_2$

$\sqrt{3}$ is irrational too
Proof:
Suppose $\sqrt{3}=\frac{m}{n}$ → integers

$\Rightarrow \gcd(m,n)=1$
$\Rightarrow (\sqrt{3})^2=\frac{m^2}{n^2}$ $\quad 3=\frac{m^2}{n^2}$ $\quad 3n^2=m^2$

$3 \mid m \cdot m \Rightarrow 3 \mid m$ (m divisible by 3)

$m=3m_1$
$3n^2=m^2=(3m_1)^2=9m_1^2$
$3n^2=9m_1^2$
$n^2=3m_1^2$
$3 \mid n \cdot 1 \Rightarrow 3n$?

$3 \mid m$ & $3 \mid n \Rightarrow \gcd(m,n) \neq 1$
$\Rightarrow$ contradiction $\Rightarrow \sqrt{3}$ irrational

$\sqrt{10}, \sqrt{15}, \sqrt{6}, \sqrt{10/3}$ ... is irrational

Claim: $\sqrt{\frac{3}{10}}$ is irrational

Proof:
Assume $\sqrt{\frac{3}{10}}=\frac{m}{n}$, $\gcd(m,n)=1$

$$\left(\sqrt{\frac{3}{10}}\right)^2=\left(\frac{m}{n}\right)^2 \Rightarrow 3n^2=10m^2=10(3m_1)^2=10\cdot 9m_1^2$$

$3n^2=10\cdot 9m_1^2$

$3 \mid n^2 \Rightarrow 3 \mid n \Rightarrow 3 \mid m$ & $3 \mid n \Rightarrow \gcd(m,n) \neq 1$

Claim: $\sqrt[3]{2}$ is irrational
Proof:
Assume rational $\Rightarrow \sqrt[3]{2}=\frac{m}{n}$ $\gcd(m,n)=1$

$$(\sqrt[3]{2})^3=\left|\frac{m}{n}\right|^3=\frac{m^3}{n^3}$$

$\Rightarrow 2=\frac{m^3}{n^3}$, $2n^3=m^3$

$\Rightarrow 2 \mid m \Rightarrow n=2m_1$

$2n^3 = m^3 = |2n_1|^3 = 8m_1^3$

$n^3 = 4m_1^3 \Rightarrow 2|n \Rightarrow 2|m$ & $2|n$ contradiction

Claim: $\sqrt{2}+\sqrt{3}$ is irrational

Proof:
Suppose $\sqrt{2}+\sqrt{3} = q = \frac{m}{n}$ rational
$(\sqrt{2}+\sqrt{3})^2 = q^2$
$2+3+2\sqrt{6} = q^2$

$\Rightarrow \frac{q^2-5}{2} = \sqrt{6}$

If q rational $\Rightarrow \frac{q^2-5}{2}$ is rational

$\Rightarrow$ $\sqrt{6}$ is rational $\Rightarrow$ false
contradiction (need to be proved)

Claim: $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational too
Proof:
Suppose $q = \sqrt{2}+\sqrt{3}+\sqrt{5}$ rational ...

Claim: $\sqrt{n}$ is rational unless n is a complete square ($n = m^2$), $n \in N$
$4 = 2^2$
$9 = 3^2$ > complete square

Rational Roots Theorem

Consider an equation of the form:
$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_0, \cdots a_n$ are integers

$x^3 - 2x^2 + 1 = 0$ any rational roots?
if $\frac{p}{q}$ is a rational root $\Rightarrow$ $p|1$ $\Rightarrow$ $p = \pm 1$ $\Rightarrow$ $\frac{p}{q} = \pm 1$
$(p,q)=1$ $q|1$ $q = \pm 1$

$x=1$, $1^3 - 2\cdot 1^2 + 1 = 1-2+1 = 0$
$x=-1$, $(-1)^3 - 2(-1)^2 + 1 = -1-2+1 = -2 \neq 0$
$\Rightarrow x=1$ is the only rational root of $x^3 - 2x^2 + 1 = 0$

$$a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0$$

$$\Rightarrow a_n p^n + a_{n-1}p^{n-1}q^1 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

$$\Rightarrow p\underbrace{(a_n p^{n-1} + \cdots + a_1 q^{n-1})}_{d''} + a_0 q^n = 0$$

$pd + a_0 q^n = 0$

$pd = -a_0 q^n \Rightarrow p \mid a_0 q^n$ let $\gcd(p, q) = 1$

$\Rightarrow p \mid a_0$ $\Rightarrow \gcd(p, q^n) = 1$

$a_n p^n + q(\cdots) = 0$

$a \mid a_n p^n \Rightarrow q \mid a_n$