Feb 11th

RSA

Public key crypto

Setup: Pick p and q distinct primes

$n=pq$

$\varphi(n)=(p-1)(q-1)$

Pick E s.t. $1<E<\varphi(n)$

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

$n=5\times 7$

$\varphi(n)=24$

Alice broadcasts (E,N)

Solve $DE\equiv 1 \bmod p$

$\equiv 1+K\varphi(N)$

Encrypt:

Bob Take M

Compute $C=M^E \bmod N$

Broadcast C

Decrypt:

Alice computes

$C^D=(M^E)^D=M^{ED}=M^{1+K\varphi(N)}=M\cdot 1 \bmod \varphi(N)$

If you have E,N,C

Find $DE\equiv 1 \bmod \varphi(N)$. Need $\varphi(N) \rightsquigarrow$ finding p & q.

Given N,E, Compute D

$N=5\cdot 7$

$E=5$, $C=17$

$\varphi(N)=24$

$ED\equiv 1 \bmod 24$

$5D\equiv 1 \bmod 24$

$\Rightarrow D=5$

$M\equiv C^D\equiv 17^5 \bmod 24$

$(E,N)=(17,3233)$

$C=2753 \Rightarrow M=?$

Claim: If $\gcd(a_1,a_2)=1$

then $\gcd(a_1a_2,b)=\gcd(a_1,b)\gcd(a_2,b)$

$\gcd(x,y)=(x,y)$ $\quad (x,y)=\max\{d: d|x, d|y\}$

$A=B$ $\begin{cases} A|B \quad B|A \\ A\le B, B\le A \end{cases}$

If $p^k|a_1a_2$ and $p^k|b$

then $p^k|a_1$, or $p^k|a_2$

Sps $p^m | a_1$, $p^n | a_2$

$m+n=k$

If $mn \neq 0$ then $p | a_1$ & $p | a_2$

contradicting $(a_1, a_2) = 1$

writing $a_1 = p_1^{e_1} \cdots p_m^{e_m}$

$a_2 = q_1^{f_1} \cdots q_n^{f_n}$

$b = r_1^{g_1} \cdots r_l^{g_l}$

p_i, q_i, r_i prime

$(a_1 a_2, b)$

If $p^k | a_1 a_2$ then

$p^k | a_1$ or $p^k | a_2$

If $p^k | a_1 a_2$ and $p^k | b$

then $p^k | (a_1, b)$ OR $p^k | (a_2, b)$

Thus $(a_1 a_2, b) | (a_1, b)(a_2, b)$

If $k_1 | a_1$ $k_1 | b$

$k_2 | a_2$ $k_2 | b$

Want $k_1 k_2 | a_1 a_2$ free

$k_1 k_2 | b$

If $k_1 | a_1$ then

$k_2 | a_2$

$\gcd(k_1, k_2) = 1$

since $\gcd(a_1, a_2) = 1$

Thus $k | a_1$, and $k | a_2$

thus $k = 1$