Recall Corollary to FLT: If $p \nmid a$ and $r \equiv s \mod p-1$ then $a^r \equiv a^s \mod p$

Last Time: Let p be a prime, e an integer satisfying

$$1 < e < p-1 \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

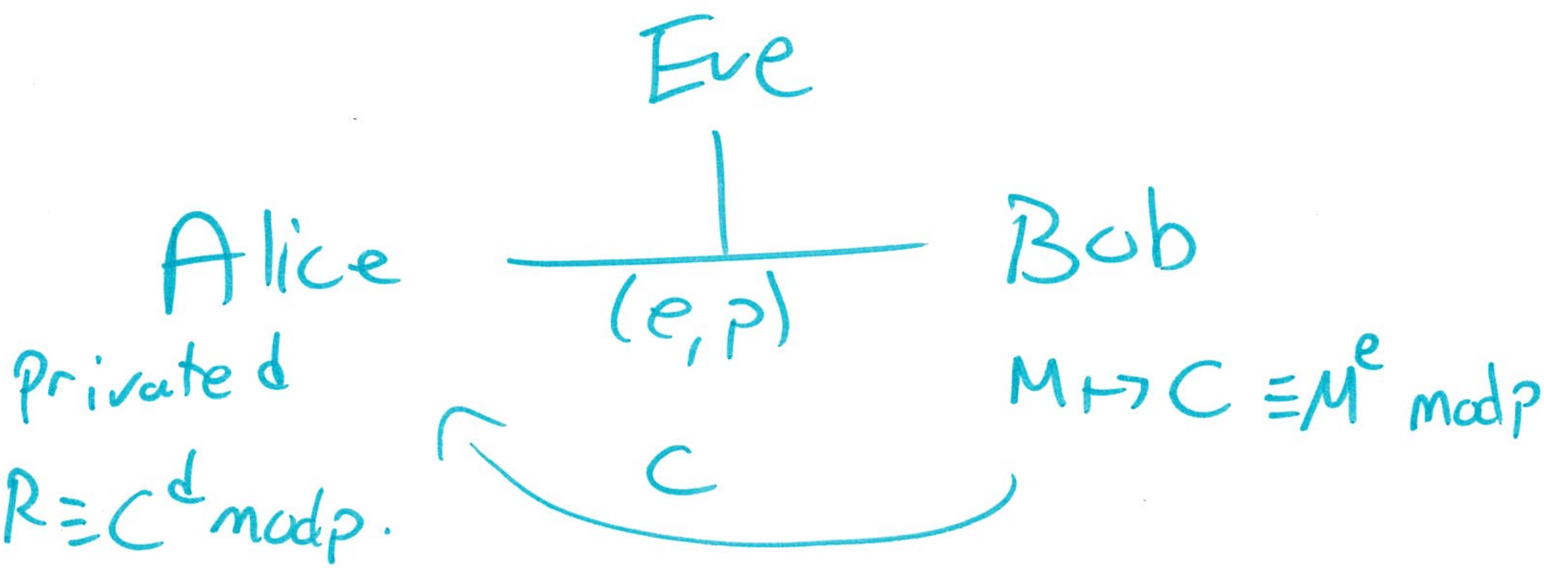
Let d be an integer such that

$$1 < d < p-1 \qquad \text{and} \qquad ed \equiv 1 \mod p-1$$

Let M be an integer between 0 and $p-1$ inclusive. Compute C an integer satisfying

$$0 \leq C < p \qquad \text{and} \qquad C \equiv M^e \mod p.$$

and let $R \equiv C^d \mod p$ be an integer with $0 \leq R \leq p-1$.



Proposition 1: $R \equiv M \mod p$.

Corollary: $R = M$

Pf of proposition 1:

If $p \mid M$ then $M = 0$. Since $0 \leq M \leq p-1$

Then $C \equiv M^e \equiv 0 \mod p$ and so $C = 0 \because 0 \leq C < p$.

Then $R \equiv C^d \equiv 0 \mod p$ and so $R = 0 \because 0 \leq R < p$.

If $p \nmid M$ then

$$
\begin{aligned}
R &\equiv C^d \mod p \\
&\equiv (M^e)^d \mod p \quad \left(\text{Recall } ed \equiv 1 \mod p-1\right) \\
&\equiv M^{ed} \mod p \\
&\equiv M \mod p \quad (\text{By corollary to FlT})
\end{aligned}
$$

Pf of Corollary: Since $0 \leq R, M \leq p-1$, and $p \mid R-M$, we have that $R-M = 0$ ie $R = M$.

RSA

Alice chooses distinct primes p & q and an integer e satisfying

$$1 < e < (p-1)(q-1) \quad \& \quad \gcd(e,(p-1)(q-1))=1$$

Alice's private key d is an integer satisfying

$$1 < d < (p-1)(q-1) \quad \& \quad ed \equiv 1 \bmod (p-1)(q-1)$$

Bob wants to send a message M, an integer between 0 & $pq-1$ inclusive. He computes C an integer satisfying

$$0 \leq C < pq \quad \text{and} \quad C \equiv M^e \bmod pq$$

Alice computes $R \equiv C^d \bmod pq$ with $0 \leq R \leq pq-1$.

Eve

Alice ———— Bob

(e, pq)

private d

$C \equiv M^e \bmod pq$

C

Compute $R \equiv C^d \bmod pq$.

Proposition 2: $R = M$

Pf: Since $ed \equiv 1 \bmod (p-1)(q-1)$, transitivity of divisibility says

$$ed \equiv 1 \bmod p-1 \;\&\; ed \equiv 1 \bmod q-1$$

Since $\gcd(e, (p-1)(q-1)) = 1$, GCDPF states that $\gcd(e, (p-1)) = 1 = \gcd(e, (q-1))$

Since $C \equiv M^e \bmod pq$ (SM) states

$$C \equiv M^e \bmod p \;\&\; C \equiv M^e \bmod q.$$

Similarly, by (SM), $R \equiv C^d \bmod p$ & $R \equiv C^d \bmod q$

By Proposition 1:

$$R \equiv M \bmod p \qquad \& \; R \equiv M \bmod q$$

By (SM) or (CRT) we have

$$R \equiv M \bmod pq$$

BUT since $0 \leq R, M \leq pq-1$ we have that $R = M$. ∎.

Why is this more secure?

Before: Given (e,p) we can easily compute $p-1$. Hence can easily compute $d \equiv e^{-1} \bmod p-1$

Now: Given (e,pq) we cannot easily compute $(p-1)(q-1)$ UNLESS we factor pq.

Notes: We denote $n=pq$ and
$$\phi(n) = (p-1)(q-1)$$
(ϕ is called Euler's toitent function or phi-function)

$$\sum_{\substack{p \leq x \\ p \text{ is prime.}}} 1 \sim \frac{x}{\log(x)}$$ PRIME NUMBER THEOREM

Let $p = 2$, $q = 11$ and $e = 3$

1. Compute n, $\phi(n)$ and d.
2. Compute $C \equiv M^e \mod n$ when $M = 8$
3. Compute $M \equiv C^d \mod n$ when $C = 6$

1. $n = 22$ $\quad \phi(n) = (2-1)(11-1) = 10$

$3d \equiv 1 \mod 10$

$d \equiv 7 \mod 10$ so $d = 7$.

2. $C \equiv M^e \mod 22$
$\equiv 8^3 \mod 22$
$\equiv 8 \cdot 64 \mod 22$
$\equiv 8(-2) \mod 22$
$\equiv -16 \mod 22$
$\equiv 6 \mod 22$.

3. $M \equiv C^d \mod 22$
$\equiv 6^7 \mod 22$
$\equiv 6 \cdot (6^3)^2 \mod 22$
$\equiv 6 \cdot (216)^2 \mod 22$
$\equiv 6(-4)^2 \mod 22$
$\equiv 6 \cdot 16 \mod 22$
$\equiv 6(-6) \mod 22$
$\equiv -36 \mod 22$
$\equiv 8 \mod 22$.