From last time

If given a, b, n integers

Solve for x $\quad ax \equiv b \pmod{n}$

1. find k & l s.t. $ka + ln = \gcd(a,n)$
2. multiply both sides of $ax \equiv b \pmod{n}$ by k.

Euler ϕ function and if $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

then $\phi(n) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_k^{a_k} - p_k^{a_k - 1})$

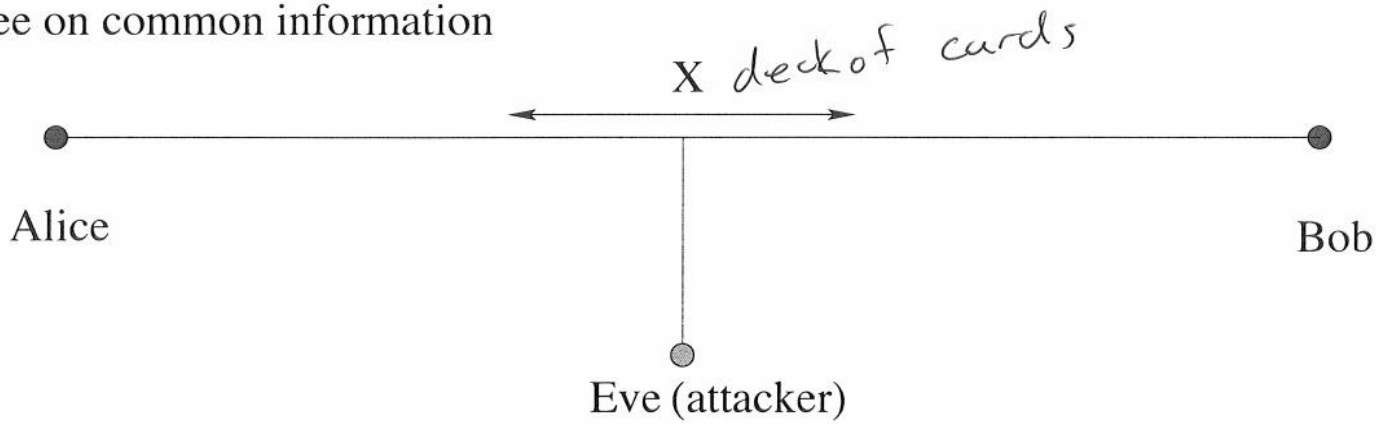
Euler-Fermat theorem says if $\gcd(a,n) = 1$

then $\quad a^{\phi(n)} \equiv 1 \pmod{n}$

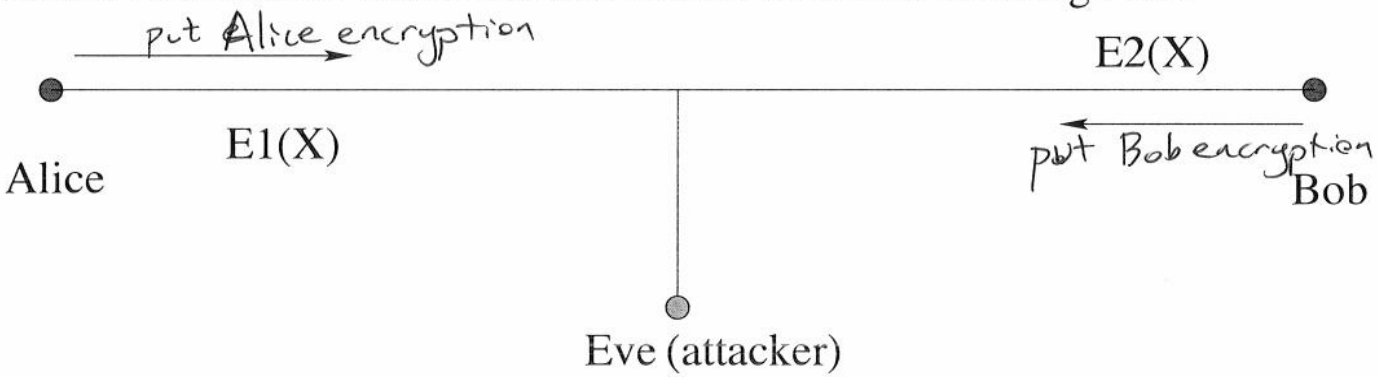
Raise a to a large power $\pmod{n}$

Abstract of Diffie–Hellman key exchange

Step 1: agree on common information



Step 2: Alice and Bob choose secret transformation of X and exchange that



Step 3: Alice and Bob create a common piece of information which can be used as a key

Alice calculates E1(E2(X))

Bob calculates E2(E1(X)) = E1(E2(X))

Eve has X, E1(X) and E2(X) but has no idea how to put them together to get E1(E2(X)) = E2(E1(X))

Diffie-Hellman Public Key Exchange

1. People $P_1, P_2, \ldots P_k$ agree on a modulus p in which they agree to do their calculations.

2. They also agree on a common base, a, which must be a primitive root of p

3. Each person P_i secretly selects a number, S_i, from 1 to $p-1$ and publicly announces the value $\beta_i = a^{S_i} \bmod p$. Eve knows a, p

P_1 picks secret S_1 $\quad a^{S_1} \pmod p$

P_2 picks secret S_2 $\quad a^{S_2} \pmod p$

P_1 & P_2 calculate $(a^{S_1})^{S_2} \equiv (a^{S_2})^{S_1} \pmod p$

base a key on this number.

$$3^{966} \pmod{143}$$

Method 1 (mod 143)

$3^2 \equiv 9$

$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81$

$3^8 \equiv 126$

$3^{16} \equiv 3$

$3^{32} \equiv 9$

$3^{64} \equiv 81$

$3^{128} \equiv 126$

$3^{256} \equiv 3$

$3^{512} \equiv 9$

$966 = 512 + 454$

$= 512 + 256 + 198$

$= 512 + 256 + 128 + 70$

$= 512 + 256 + 128 + 64 + 4 + 2$

$3^{966} \equiv 3^{512} \cdot 3^{256} \cdot 3^{128} \cdot 3^{64} \cdot 3^{4} \cdot 3^{2}$

$\equiv 9 \cdot 3 \cdot 126 \cdot 81 \cdot 81 \cdot 9$

$\equiv 81 \cdot 9 \equiv 14 \pmod{143}$

Method 2 (mod 143

$3^{966} \equiv (3^{483})^2 \equiv 14$

$3^{483} \equiv 3 \cdot 3^{482} \equiv 27$

$3^{482} \equiv (3^{241})^2 \equiv 9$

$3^{241} \equiv 3 \cdot 3^{240} \equiv 3$

$3^{240} \equiv (3^{120})^2 \equiv 1$

$3^{120} \equiv (3^{60})^2 \equiv 1$

$3^{60} \equiv (3^{30})^2 \equiv 1$

$3^{30} \equiv (3^{15})^2 \equiv 1$

$3^{15} \equiv 3 \cdot 3^{14} \equiv 1$

$3^{14} \equiv (3^{7})^2 \equiv 48$

$3^{7} \equiv 3 \cdot 3^{6} \equiv 42$

$3^{6} \equiv (3^{3})^2 \equiv 14$

$3^{3} \equiv 27$

Method 3

$3^{\phi(143)} \equiv 1 \pmod{143}$

$143 = 11 \cdot 13$

$\phi(143) = 10 \cdot 12$

$= 120$

$966 = 8 \cdot 120 + 6$

$3^{966} \equiv (3^{120})^8 \cdot 3^6$

$\equiv 3^6 \pmod{143}$

$\equiv 14$

Example

$$7^{359} \equiv 7^{360-1} \pmod{143}$$

$$\equiv 7^{360} \cdot 7^{-1} \pmod{143}$$

$$\equiv 7^{-1} \equiv 41 \pmod{143}$$

$$7 \cdot k \equiv 1 \pmod{143}$$

then $k \equiv 7^{-1} \pmod{143}$

$143 = 7 \cdot 20 + 3 \qquad 143 - 7 \cdot 20 = 3$

$7 = 3 \cdot 2 + 1 \quad \Rightarrow \quad 7 - 3 \cdot 2 = 1$

$$7 - (143 - 7 \cdot 20) \cdot 2 = 1$$

$41 \cdot 7 \equiv 1 \pmod{143} \Leftarrow 41 \cdot 7 - 2 \cdot 143 = 1$

I want people to send me a message.

Pick p, q, e and I hold these secret.

Publish $p \cdot q = n$ and a number d such that $d \cdot e \equiv 1 \pmod{\phi(n)}$

I am the only person that has $\phi(n)$ and e so I am the only person that has d. But I give that away.

Factoring n is sufficient to recover $\phi(n)$ and e because $\phi(n) = (p-1)(q-1)$

and $e \equiv d^{-1} \pmod{\phi(n)}$

$d \cdot e = 1 + k\phi(n) \Leftarrow d \cdot e \equiv 1 \pmod{\phi(n)}$

Person who wants to send me a message computes $m^d \equiv c \pmod{n}$

to decrypt $c^e \equiv m^{d \cdot e} \equiv m^{1 + k\phi(n)} \equiv m^1 \cdot (m^{\phi(n)})^k \equiv m \pmod{n}$

Solving Congruences

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	10	9	7	3	6	1

Example 1: Solve $9x = 5 \bmod 11$. $9 \equiv 2^6 \quad 5 \equiv 2^4 \pmod{11}$

Letting $x = 2^y$, we have let $x \equiv 2^y \pmod{11}$

$$9 \cdot x \equiv 2^{6+y} \equiv 2^6 2^y \equiv 9x \equiv 5 \equiv 2^4 \bmod 11$$

and $2^{6y+10k} \equiv (2^{10})^k 2^{6+y} \equiv 2^4 \pmod{11}$ $y \equiv -2$ solves the equation

$$6 + y \equiv 4 \bmod \varphi(11).$$

Therefore $6+y+10k = 4$ OR $2^{10} \equiv 2^0 \equiv 1 \pmod{11}$

$$y = 8 \Rightarrow x = 2^8 = 3.$$ $2^{-12} \equiv 2^{-2} \equiv 2^8 \equiv 2^{18}$

Example 2: Solve $7^x = 5 \bmod 11$.

Since 2 is a primitive root, we have

$$2^{7x} = (2^7)^x = 7^x = 5 = 2^4 \bmod 11$$

Therefore

$$7x = 4 \bmod \varphi(11) \Rightarrow x = 2.$$

Using powers of a primitive root I can also compute x in an equation of the form $a^x \equiv b \pmod{n}$