Diffie-Hellman Key Exchange

Alice & Bob agree on prime p and $b \in \mathbb{N}$
Eve sees p & b.

Alice

picks s, $1 < s < p-1$
computes $S = b^s \% p$
sends S to Bob (littles)
computes $K = T^s \% p$
uses K as secret key

Bob

picks t, $1 < t < p-1$
computes $T = b^t \% p$
sends T to Alice
computes $K = S^t \% p$
uses K as secret key

Example: $p = 163$ $b = 11$
Alice picks $s = 13$
Bob picks $t = 23$

Alice:

$S = 11^{13} \% 163$
$= 19$
$K = 116^{13} \% 163$
$= 154$

Bob:

$T = 11^{23} \% 163$
$= 116$
$K = 19^{23} \% 163$
$= 154$

Theorem Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$ where

$$a \equiv b \pmod{m}$$

and

$$c \equiv d \pmod{m},$$

then $a + c \equiv b + d \pmod{m}$

& $a \cdot c \equiv b \cdot d \pmod{m}$

Proof: We have

$b = a + sm$ & $d = c + tm$

for some s & $t \in \mathbb{Z}$.

$$\begin{aligned} b + d &= (a + sm) + (c + tm) \\ &= (a + c) + (s + t)m \end{aligned}$$

Hence $(b+d) \% m = (a+c) \% m$ and

$a + c \equiv b + d \pmod{m}$

Similarly

$$\begin{aligned} bd &= (a + sm)(c + tm) \\ &= ac + atm + scm + stm^2 \\ &= ac + (at + sc + stm) \cdot m \end{aligned}$$

Thus, $bd \equiv ac \pmod{m}$

$\boxtimes$

Repeated Squaring

Bob ~~Alice~~ wants to compute $11^{23} \% 163$

$11^{23} = 895430243255237372246531$

We don't need 11^{23} to find $11^{23} \% 163$.

$23 = 10111$ in base 2

$$11^{23} = 11^{16+4+2+1} = 11^{16} \cdot 11^4 \cdot 11^2 \cdot 11$$

$11 \% 163 = 11$
$11^2 \% 163 = 121 \% 163 = 121$
$11^4 \% 163 = (121 \cdot 121) \% 163 = 14641 \% 163 = 134$
$11^8 \% 163 = (134 \cdot 134) \% 163 = 17956 \% 163 = 26$
$11^{16} \% 163 = (26 \cdot 26) \% 163 = 676 \% 163 = 24$

$11^{23} \% 163 = (24 \cdot 134 \cdot 121 \cdot 11) \% 163$

$= [((24 \cdot 134) \% 163) \cdot ((121 \cdot 11) \% 163)] \% 163$

$= [(3216 \% 163)(1331 \% 163)] \% 163$

$= (119 \cdot 27) \% 163$

$= (3213) \% 163 = 116$

RSA Public-Key Cryptography

1. Secretly pick 2 prime numbers p & q
2. Let $n = p \cdot q$ and let $\phi(n) = (p-1) \cdot (q-1)$.
3. Pick e and d s.t. $1 < e < \phi(n)-1$ & $1 < d < \phi(n)-1$ and $e \cdot d \equiv 1 \pmod{\phi(n)}$
4. Publish e and n as your public key. Keep d, p & q secret.

Encryption To encrypt message M, $0 \leq M \leq n-1$

$$C = M^e \,\%\, n$$

Decryption

$$P = C^d \,\%\, n$$

Claim: $M^{ed} \equiv M \pmod{n}$

RSA example:

$p=7 \quad q=11$

$\phi(n) = 6 \cdot 10 = 60$

$e=13 \quad d=37$

Check that $13 \cdot 37 = 481 \equiv 1 \pmod{60}$

Secret key: $d=37$ $p=7$ & $q=11$

Public key: $e=13$, $n=77$

Encrypt M=5

$5^{13} \% 77 = 1220703125 \% 77 = 26$

Decrypt c=26

$26^{37} \% 77 = \ldots = 5$

Multiplication mod 7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Multiplication mod 6

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication table for

$\mathbb{Z}_{15}^* = \{x \in \mathbb{Z}_{15} \mid \gcd(x, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1