Alice & Bob agree on $5 \pmod{17}$

a b

$5^a \longrightarrow$ send to Bob

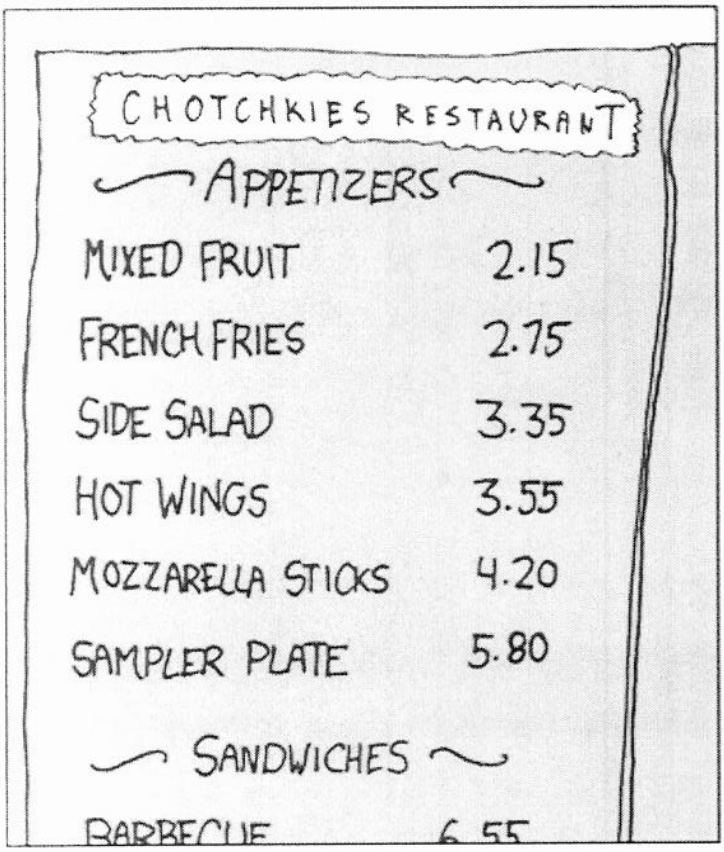
$5^b \longrightarrow$ sends to Alice

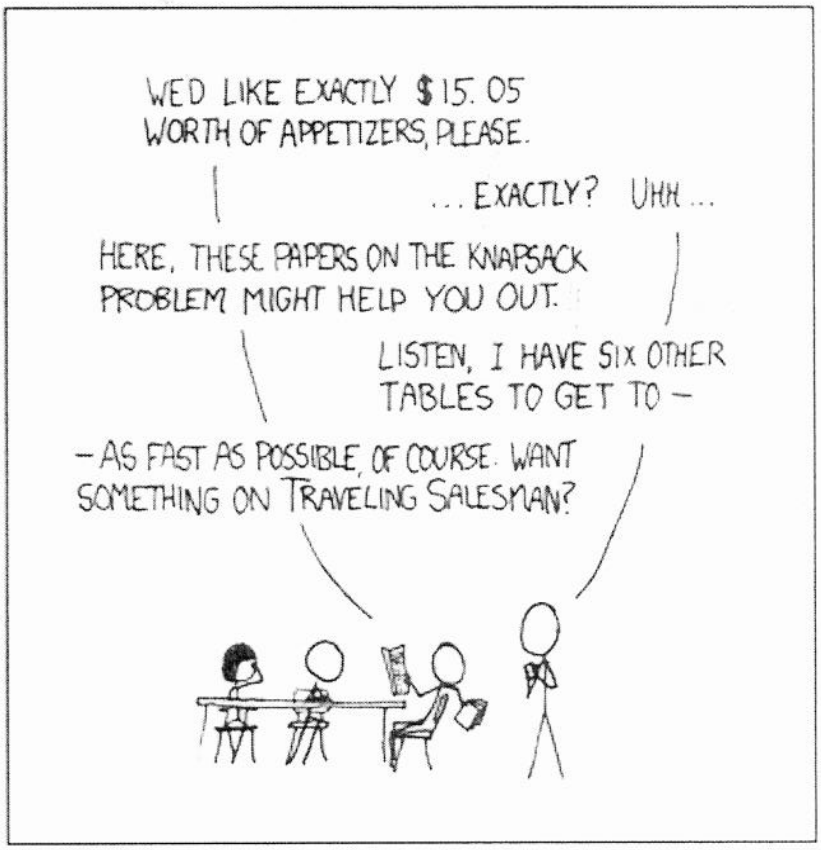
$(5^b)^a \equiv (5^a)^b$

Alice
calculate

MY HOBBY:

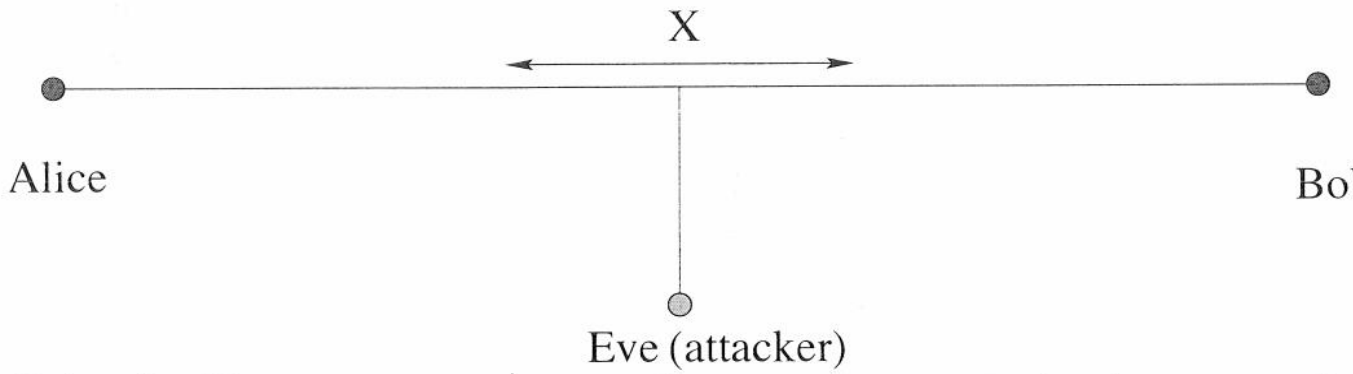
EMBEDDING NP-COMPLETE PROBLEMS IN RESTAURANT ORDERS





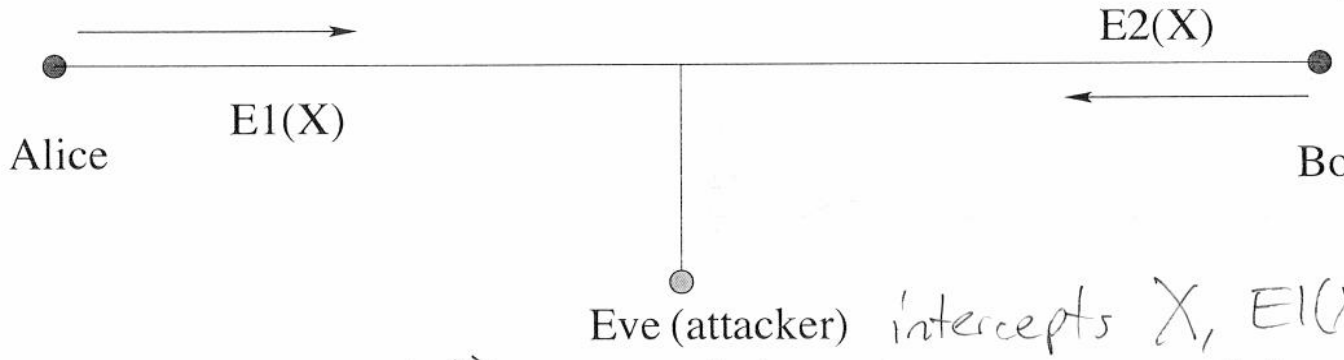
Abstract of Diffie–Hellman key exchange

Step 1: agree on common information



E1 & E2 are transformations which can be done in either order with same result.

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



intercepts X, E1(X), E2(X)

Bob calculates E2(E1(X))

Alice calculates E1(E2(X))

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))

$$x \equiv 2^y \pmod{11}$$

$$9 \equiv 2^6 \pmod{11}$$

$$5 \equiv 2^4 \pmod{11}$$

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

$$2^{6+y} \equiv 2^4 \pmod{11}$$

~~$6+y \equiv 4 \pmod{11}$~~

$$2^{10} \equiv 1 \pmod{11}$$

$2^{6+y} \cdot (2^{10})^k \equiv 2^4 \pmod{11}$ for any k.

$6+y+10k = 4 \iff 6+y \equiv 4 \pmod{10}$

$y \equiv -2 \equiv 8 \pmod{10}$

$y \equiv 8 \pmod{10}$ $\quad x = 2^8 \equiv 3 \pmod{11}$

$9 \cdot 3 \equiv 27 \equiv 5 \pmod{11}$

Primitive Roots

Definition: Given a prime p, an integer a is said to be a *primitive root* mod p if the numbers

$$a^1, a^2, a^3, \ldots, a^{p-1}$$

are all distinct mod p.

Example 1: 2 is a primitive root mod 11.

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

Example 2: 3 is *not* a primitive root mod 11.

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

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 $9x = 5 \mod 11$.
Letting $x = 2^y$, we have

$$2^{6+y} = 2^6 2^y = 9x = 5 = 2^4 \mod 11$$

and

$$6 + y = 4 \mod \varphi(11).$$

Therefore

$$y = 8 \quad \Rightarrow \quad x = 2^8 = 3.$$

Example 2: Solve $7^x = 5 \mod 11$.
Since 2 is a primitive root, we have

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

Therefore

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

powers of 8 mod 37

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
8	27	31	26	23	36	29	10	6	11	14	1	8	27	31	...

$$17 \cdot x \equiv 23 \pmod{37}$$
$$2^7 \cdot 2^y \equiv 2^{15} \pmod{37}$$
$$\Rightarrow 7 + y \equiv 15 \pmod{36}$$
$$\Rightarrow y \equiv 8 \pmod{36}$$
$$\Rightarrow x \equiv 2^8 \equiv 34 \pmod{37}$$

$$x^5 \equiv 6 \pmod{37}$$
$$2^{5y} \equiv (2^y)^5 \equiv 2^{27} \pmod{37}$$
$$-y \equiv 7 \cdot 5y \equiv 7 \cdot 27 \equiv 7 \cdot (-9) \pmod{36}$$
$$y \equiv 63 \equiv 27 \pmod{36}$$
$$x \equiv 6 \equiv 2^{27} \pmod{37}$$

$$x^5 \equiv 6^2)^2 \cdot 6 \equiv (-1)^2 \cdot 6 \equiv 6 \pmod{37}$$

If a is a primitive root $\pmod p$, then a^x is also a primitive root if x is relatively prime to $p-1$

---

if a is a primitive root then for any $b \in \{1, \ldots, p-1\}$
$\exists\, y$ s.t. $a^y \equiv b \pmod p$

Claim: $c \equiv a^x \pmod p$ where $\gcd(x, p-1) = 1$ is also a primitive root

$$c^z \equiv b \pmod p$$
$$(a^x)^z \equiv a^y \pmod p$$
$$a^{xz} \equiv a^y \pmod p$$
$$\iff xz \equiv y \pmod{(p-1)}$$

since $\gcd(x, p-1) = 1$ there is a solution to this eq.

$z \equiv (x)^{-1} y \pmod{p-1}$ $\therefore$ c is a prim. root.

$8^4 \equiv (2^3)^4 \equiv 2^{12}$ $\quad 8^5 \equiv (2^3)^5 \equiv 2^{15}$

Public Key Exchange: An Example

Given p, if there is at least one primitive root, how many other primitive roots are there?

Powers of 2 mod 37

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^s	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2^s	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1

$\phi(36) = 3^2 \cdot 2^2 = (3^2-3)(2^2-2) = 12$

Powers of 17 mod 37

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
17^s	17	30	29	12	19	27	15	33	6	28	32	26	35	3	14	16	13	36

s	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
17^s	20	7	8	25	18	10	22	4	31	9	5	11	2	34	23	21	24	1

Say that *Alice* and *Bob* wish to communicate after agreeing on on a public modulus 37 and a primitive root 17. *Alice* also chooses a secret key 9 and so she sends $17^9 \equiv 6 \ (mod\ 37)$ to *Bob*. At the same time *Bob* chooses 10 as his secret key and so he sends $17^{10} \equiv 28 \ (mod\ 37)$ to *Alice*. *Alice* and *Bob* do not know each others secret keys but they *do* know $17^{\text{secret key}} \ (mod\ 37)$.

The common key to *Alice* and *Bob* is

$$6^{10} = 17^{9\times 10} = 28^9 \bmod 37$$

$36 \equiv$

$17^{90} \equiv 17^{18}$

$90 = 2 \cdot 36 + 18$

ElGamal Public Key System

a secret Bob

To send a message X to **Bob** using his public key β. **Alice** chooses at random a secret number S_A in the interval $\{1, \ldots, p-1\}$, and sends the pair

$$(Y, Z)$$

where

$$Y := a^{S_A} \bmod p. \quad \text{and} \quad Z := X\,\beta^{S_A} \bmod p$$

Bob can then get X back using his secret exponent S_B:

$$X \equiv Z\,(Y^{S_B})^{-1} \bmod p.$$

In this, we can consider that Y is used to "encode" S_A.

$\left(\left(a^{S_A}\right)^{S_B}\right)^{-1}$

$X \cdot \beta^{S_A} \equiv X \left(a^{S_B}\right)^{S_A}$

Baby step/Giant step method

Goal: Solve $a^x \equiv b \pmod{n}$.

Idea: Find $a^i \equiv ba^{-j} \pmod{n}$ by searching through a small enough space of possible i and j.

Fix $m = \lceil \sqrt{(\phi(n))} \rceil$ then find $c \equiv a^{-m} \pmod{n}$.

Next calculate a table of $a^i \pmod{n}$ for $0 \leq i < m$ and then calculate $bc^j \pmod{n}$ for $0 \leq j < m$ until you find one of these values in the table.

Solution: When we find $a^i \equiv bc^j \pmod{n}$ then we have $a^{i+mj} \equiv a^i c^{-j} \equiv b \pmod{n}$.

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 28$

$3^8 \equiv (28)^2 \equiv 42$

$3^8 \equiv (3^4)^2 \equiv ((3^2)^2)^2$

$53 = 42 + 11$ $\quad 42 = 3 \cdot 11 + 9$ $\quad 11 = 9 + 2$ $\quad 9 = 4 \cdot 2 + 1$

Example: $p = 53$ and $a = 3$. We wish to solve $3^x = 41 \pmod{53}$.

$42 \cdot 24 \equiv 1 \pmod{53}$, $3^8 = 3^{-8}$

$(3^{-m})^i \equiv (3^m)^{-1} \equiv (3^{-1})^m$

- $m = \lceil \sqrt{\phi(53)} \rceil = 8$ and $3^{-8} \equiv 24 \pmod{53}$.
- Now $41 \cdot 24^i \pmod{53}$.

$41 \cdot (3^{-8})^i$

i	$3^i \pmod{53}$	i	$41 \cdot 24^i \pmod{53}$
0	1	0	41
1	3	1	30
2	9	2	31
3	27	3	2
4	28	4	48
5	31	5	39
6	40	6	35
7	14	7	45

$m = \lceil \sqrt{\phi(53)} \rceil$

$x \equiv i \cdot m + j \pmod{\phi(53)}$

$0 \leq i < m, \quad 0 \leq j < m$

- Conclusion: $3^{2 \cdot 8 + 5} \equiv 3^{21} \equiv 41 \pmod{53}$

$3^5 \equiv 41 \cdot (3^{-8})^2$ $\quad 41 \equiv 3^{5+8+8} \equiv 3^{21}$