PUBLIC KEY CRYPTOGRAPHY

MTH 440

Public vs. Private (symmetric) ciphers

Public (e.g. RSA)

- Key size - modulus N: 1024-2048 bits
- Cipher operations: exponentiation modulo N
- SLOW
- Keys can be made public – no private communication required (possible to do over internet)

Private (e.g. AES)

- Key size : 128, 192 or 256 bits
- Cipher operations: shifts, rotates, xor, etc.
- FAST
- Keys must be exchanged over a private network (impossible to do over the internet)

Best of both worlds…

- Use a public key cipher to exchange a private key
- Use the symmetric cipher to encipher large amounts of data

A second public key exchange system: Diffie-Hellman key exchange

- The Diffie-Hellman key exchange scheme, named for Whitfield Diffie and Martin Hellman bases its security on the difficulty of the discrete logarithm problem:
- Given a modulus N, a base g, and a value y, find an x such that

$$y = g^x \bmod N$$

- Example $3 = 2^x \bmod 5$ (modulus 5, base 2, y = 3)
- Guess and check. Is it 1? Is it 2? Is it 3?
- What about $8 = 3^x \bmod 101$ (modulus 101, base 3, y = 8)
- Fact: If N is chosen "properly" and is of size at least 1024 bits (~320 decimal digits) then this problem is *computationally infeasible;*

Diffie-Hellman Key Exchange

ALICE

- Alice and Bob agree on a public modulus p (PRIME) and base g
- Alice chooses a secret a, 0<a<p and computes

$$y_a = g^a \bmod p$$

- Alice sends y_a to Bob→
- Alice computes the shared key

$$K = (y_b)^a = y^{ab} \bmod p$$

BOB

- Alice and Bob agree on a public modulus p (PRIME) and base g
- Bob chooses a secret b, 0<b<p and computes

$$y_b = g^b \bmod p$$

- ←Bob sends y_b to Alice
- Bob computes the shared key

$$K = (y_a)^b = y^{ab} \bmod p$$

Let's try it!

- Let's use a modulus of 13 and a base of 2.
- Think of a number between 2 and 12 – call it a (don't tell anyone)
- Compute 2^a mod 13 – call it y_a
- I did the same thing – my y_b is 7
- Compute $(y_b)^a$ mod 13 = 7^a mod 13

Attacks on the discrete log problem

- Guess and Check
- Divide and conquer
- Other more sophisticated attacks beyond the scope of this course….

Guess and Check

- The DL problem is to find x such that $y=g^x \bmod p$ for a large prime p when given y, g and p.
- Guess and check - does

$$g^0=y \bmod p?$$

$$g^1=y \bmod p?$$

$$\ldots g^{10} = y \bmod p$$

$$\ldots g^{p-1}=y \bmod p?$$

takes (at most p-1 guess)

Divide and Conquer

- Divide and conquer:
  - Let z be the smallest integer greater than the square root of p (note $z^2 > p$ or $z^2-1 \geq p$)
  - Let $0 \leq a_i < z$, and $0 \leq b_i < z$
  - Then all numbers between 0 and p-1 can be written as

$$a_i + b_i z$$

(Note $a_i = b_i = 0$ gives $0 + 0z = 0$,

$a_i = b_i = z-1$ gives $z-1+z-1(z)=z-1+z^2-z = z^2-1 \geq p$)

Example

- Suppose p = 101 then the square root is 10.0498…
- So z = 11, $0 \leq a_i < 11$, $0 \leq b_i < 11$
- 0+0*11 = 0, 10+10*11 = 120 so as the a_i and b_i vary, all numbers between 0 and 100 are represented

Divide and Conquer

- Given y,g and p where $y = g^x \bmod p$, find x.
- Write $x = a_i + b_i z$ where a_i, b_j, and z are as defined previously
- Note $$y = g^x = g^{a_i + b_j z} = g^{a_i} \cdot \left(g^z\right)^{b_j} \bmod p$$
- So $$y\left(\left(g^z\right)^{-1}\right)^{b_j} = g^{a_i} \bmod p$$
- Or $$y\left(g^{-z}\right)^{b_j} = g^{a_i} \bmod p$$

Divide and Conquer

- So if $x = a_i + b_i z$ then we just need to find b_j and a_i such that $$y\left(g^{-z}\right)^{b_j} = g^{a_i} \bmod p$$
- Then $x = a_i + b_j z$
- Example: $8 = 3^x \bmod 101$
- $y = 8$, $g = 3$, $p = 101$, $z = 11$,
- $g^{-z} = 3^{-11} = ((3)^{-1})^{11} = 34^{11} = 72 \bmod 101$
- So we want

$$8\left(72\right)^{b_j} = 3^{a_i} \bmod 101$$

Divide and Conquer

$$8(72)^{b_j} = 3^{a_i} \bmod 101$$

a_i, b_i	$8*(72)^{bj} \bmod 101$	$3^{ai} \bmod 101$
0	$8\cdot(72)^{0} = 8$	$3^{0}=1$
1	$8\cdot(72)^{1} = 71$	$3^{1} = 3$
2	$8\cdot(72)^{2} =$ **62**	$3^{2} =$ **9**
3	$8\cdot(72)^{3} =$ **62**$\cdot 72 =$**20**	$3^{3}=$ **9**$\cdot 3 =$ **27**
4	$8\cdot(72)^{4} =$ **20**$\cdot 72 =$**26**	$3^{4} =$ **27**$\cdot 3 =$ **81**
5	$8\cdot(72)^{5} =$ **26**$\cdot 72 =54$	$3^{5} =$ **81**$\cdot 3 = 41$
6	50	22
7	65	66
8	34	97
9	24	89
10	11	65

So in this case $b_j = 7$, $a_i=10$
Hence x = 10 + 7*11 = 87
Check: $3^{87}=8 \bmod 101$!

Try it!

- Worksheet