ECE471/571 Diffie Hellman Key Exchange

DHKE Global parameters:

q: prime modulus.

$\alpha < q$ primitive root (generator)

Alice	Bob
Choose $x_A \xleftarrow{R} \mathbb{Z}_q^*$	$x_B \xleftarrow{R} \mathbb{Z}_q^*$
public number $y_A = \alpha^{x_A} \bmod q$	$y_B = \alpha^{x_B} \bmod q$
$\xrightarrow{y_A}$	
	$\xleftarrow{y_B}$
$K_{AB} = (y_B)^{x_A} \bmod q$	$K_{AB} = (y_A)^{x_B} \bmod q$
$= (\alpha^{x_B} \bmod q)^{x_A} \bmod q$	$= (\alpha^{x_A} \bmod q)^{x_B} \bmod q$
$= \alpha^{x_B \cdot x_A} \bmod q$	$= \alpha^{x_A \cdot x_B} \bmod q$

Ex $p = 23$. $\alpha = 5$

Alice	Bob
$x_A = 6$	$x_B = 15$

$5^6 \bmod 23 = 8 \xrightarrow{8}$

$5^{15} \bmod 23 = 19$

$19^6 \bmod 23 = 2 \xleftarrow{19}$

$8^{15} \bmod 23 = 2$

Discrete logarithm (DL)

Alice $g=3$ $p=5$ Bob

$x_A = 2$ $x_B = 3$

$y_A = g^{x_A} = 3^2 \bmod 5$

$= 4$

$y_B = g^{x_B} = 3^3 \bmod 5$

$= 2$

$y_B^{x_A} = 2^2 \bmod 5$

$= 4$

$y_A^{x_B} = 4^3 \bmod 5$

$= 4$

base \ exp	x = 1	2	3	4	5	6	7	$p=7$ $\mathbb{Z}_p^*$
X	1	1	1	1	1	1	1	

	x	1	2	3	4	5	6	
✓	3	3	2	6	4	5	1	generators
X	4	4	2	1	4	2	1	
✓	5	5	4	6	2	3	1	generator
X	6	6	1	6	1	6	1	

order of element

ord(1) = 1. ord(3) = 6 ord(5) = 6

ord(2) = 3 ord(4) = 3 ord(6) = 2

when ord(a) = p-1. a is generator

$ord_p(a) \mid (p-1)$ & $\phi(p) = p-1$.

# of generators in Z_p^* = $\phi(p-1)$

$p-1=6$

$\phi(6)=2$

DLP: given y (value), g (base), p - modulus.

find x, s.t. $g^x = y \bmod p$

x is discrete log. of y, base g, mod p

e.g $y=3$. $p=7$. $g=3$ $x=1$.

$y=4$, $p=7$. $g=3$. $x=4$

non-discrete logarithm no modulus is easy

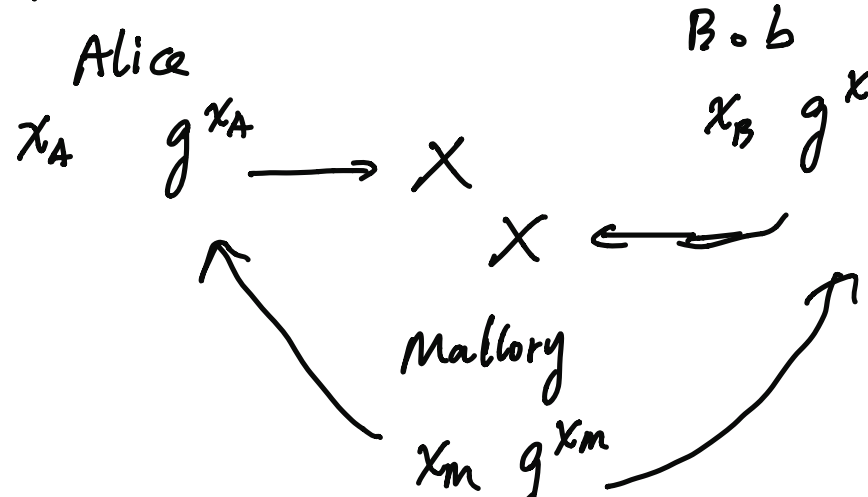
$y=9$. $g=3$. $x=2$ $\quad 3^2=9$

10

$\log_3 10 = ?$

But discrete log is hard given large p

MitM Attack



$(g^{x_m})^{x_A} \bmod p = (g^{x_A})^{x_m}_{\bmod p}$ $\quad (g^{x_m})^{x_B} \bmod p$

$(g^{x_B})^{x_m}_{\bmod p}$

K_{AM} $\quad K_{BM}$