$= 2 \cdot 5 + 1$, $q = 5$

$p = 11$
$g = 3$

$p = 11$

p a prime

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

g^1	g^2	g^3	g^4	g^5	g^6	g^7	g^8	g^9	g^{10}
3	9	5	4	1	3	9	5	4	1

$g = 3$

$g = 3$ generates $\{3, 9, 5, 4, 1\}$
a group of order 5

$20 \bmod 11$

$20/11 = 1$ remainder 9

$g = 7$

	1	2	3	4	5	6	7	8	9	10
g^1	7,	5,	2,	8,	10,	4,	6,	9,	8,	1

$g = 7$ generates
$\{7, 5, 2, 3, 10, 9, 6, 9, 8, 1\}$
$= \mathbb{Z}_p^*$

$g = 10$ $\quad g^1 = 10$

$g^2 = 1$

$= Z_p^*$.

$g = 10$

$g^1 = 10$

$g^2 = 1$

$g^3 = 10$

$g = 10$ generate

$\{10, 1\}$.

$x = 4$

$X = g^4 = 7^4 = 3$

$y = 8$

$Y = g^8 = 9$

3

9

$9^4 \bmod 11$

$(7^2)^4 \bmod 11$.

$3^8 \bmod 11 = 5$

$(7^4)^8 \bmod 11$

$x = 3, y = 9$

$g = 7, p = 11$

$X \cdot Y = 7^{4} \cdot 7^{8} = 7^{4+8}$

Attacker doesn't know x, y

$\Rightarrow$ learn x, y.

Discrete log problem:

$X \Rightarrow$ find x s.t. $g^x = X$

HARD for large p,* caveat

DDH. P, g.

x, y, g^x, g^y, ?, g^{xy}, g^r

flip a coin

H

attacker: g^x, g^y, g^{xy}

T

g^x, g^y, g^r

everything in this lecture mod n

right now: mod p.

$Z_p^* = \{1, 2, \ldots, p-1\}$

multiplication

KE

KE

AES-CTR

g^x

g^y

$k = H(g^{xy})$

$k = H(g^{xy})$

$AES\text{-}CTR_k(\ldots)$

repeat with k_2

k_2

k:

$AES\text{-}CTR_k(\ldots)$

assumes random k.

sk_A, pk_A

pk_B

sk_B, pk_B

pk_A

Pick random x

$g^x, sign_{sk_A}(g^x)$

p, q

e $\quad$ c $\quad$ d private

$m^e \bmod N \rightarrow c$

What if $m > N$

decrypt $m \bmod N$