

$$c(2 \cdot 5 + 1) \cdot g = 5$$

$$= 2 \cdot 5 + 1$$

$$p = 11$$

$$g = 3$$

$p = 11$   
 $p$  a prime

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

$g^1$	$g^2$	$g^3$	$g^4$	$g^5$	$g^6$	$g^7$	$g^8$	$g^9$	$g^{10}$
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 mod 11

20 mod 11  
 $20/11 = 1$  (remainder 9)

$$g = 7$$

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

$g = 7$  generates  
 $\{7, 5, 2, 3, 10, 4, 6, 9, 8, 1\}$   
 $= \mathbb{Z}_p^*$

$$g = 10$$

$$g^1 = 10$$

$$g^2 = 1$$

$$g = 10$$

$$g^1 = 10$$

$$g^2 = 1$$

$$g^3 = 10$$

...

$g = 10$  generates

$\{10, 1\}$

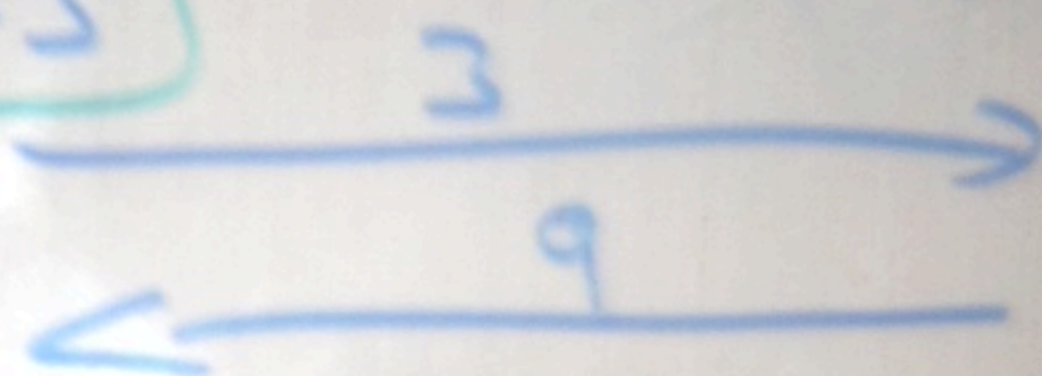
$$= \mathbb{Z}_p^*$$

$$x = 4$$

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

$$y = 9$$

$$Y = g^y = 9$$

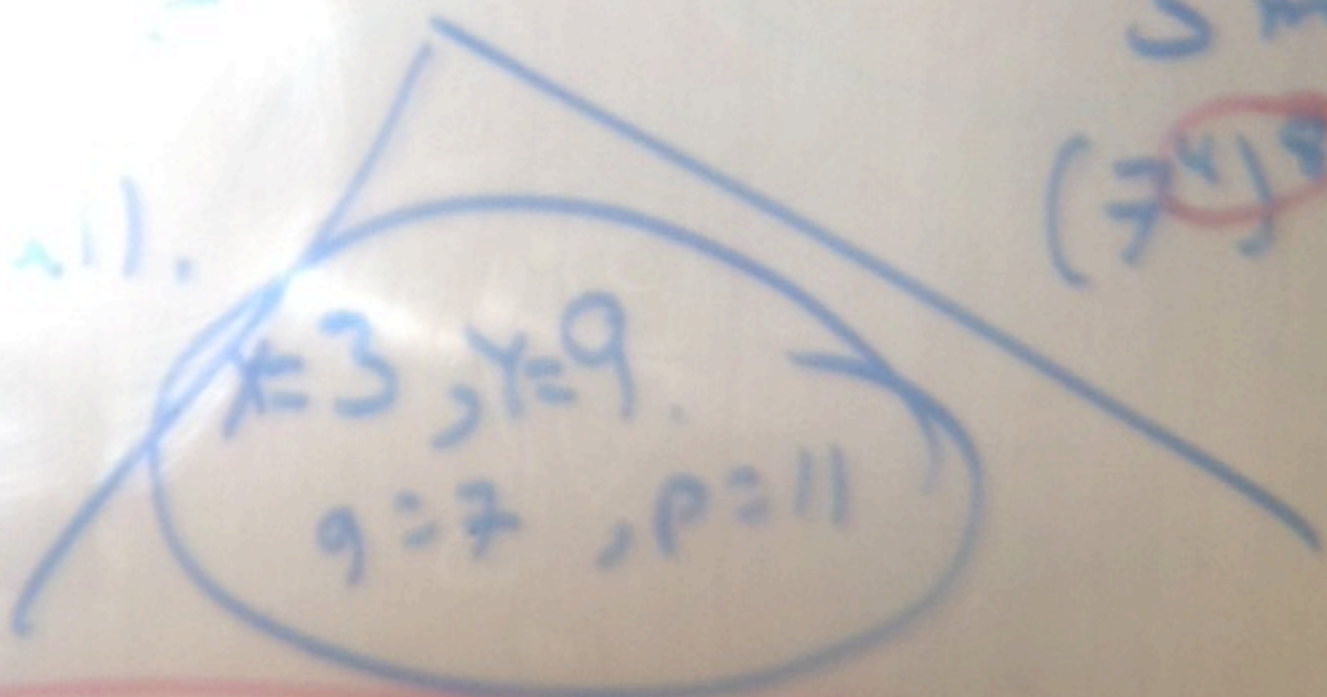


$$g^x \pmod{p}$$

$$(7^4) \pmod{11}$$

$$3^y \pmod{11} = 5$$

$$(7^9) \pmod{11}$$



$$X \cdot Y = 7^4 \cdot 7^9 = 7^{13} = 7^2 = 4$$

Attacker doesn't know  $x, y$

$\Rightarrow$  learn  $x, y$

Discrete log problem:

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

# HARD for large $P$ \* caveat

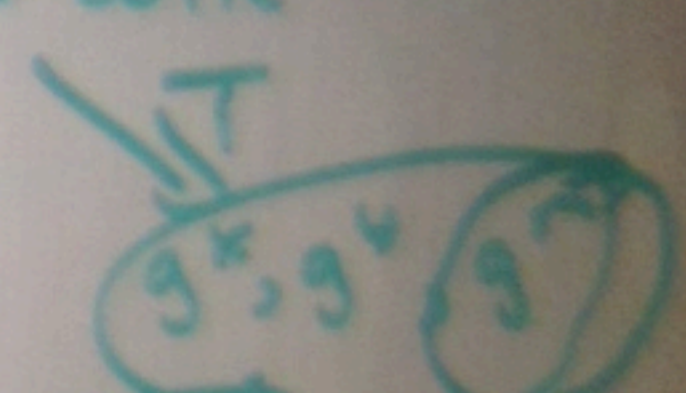
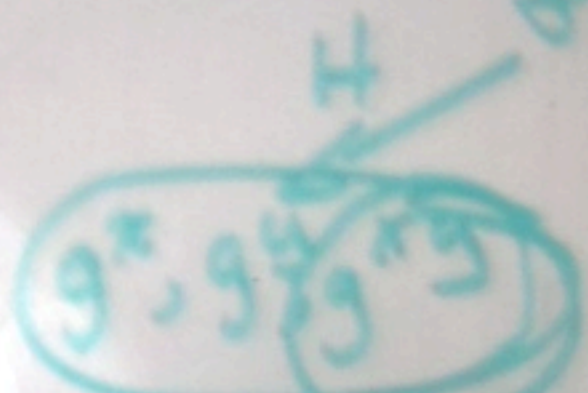
DDH.

$P, g$ .

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

flip a coin

attacker



everything in this lecture  
mod  $n$   
right now: mod  $P$ .

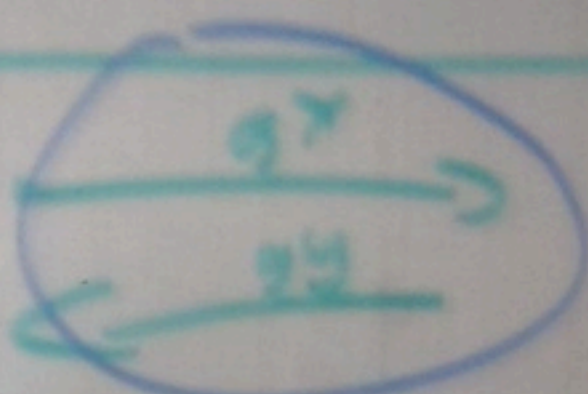
$$\mathbb{Z}_P^* = \{1, 2, \dots, P-1\}$$

multiplication

KE

$KE$

AES-CTR



$g^H(g^{10})$

$KEH(g^{19})$

AES-CTR<sub>k</sub>(...)

repeated k.

$k_i$

$k_i$

AES-CTR<sub>k</sub>(...)

assumed random k.

~~skA, pkA~~  
skA, pkA  
pkB

skB, pkB  
pkA.

pick random x  $\rightarrow$   $g^x, \text{sign}_{skA}(g^x)$

$\leftarrow$

$p, q$

$e$  public

$d$  private

$m^e \pmod N \rightarrow c$

What if  $m > N$ ?

decrypt  $m \pmod N$