Example: In the video looked at eg. $2^{13} \bmod 29$

$2^{18} \bmod 29$, etc.

$2^{13} \bmod 29$

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ mod

$2 \cdot 2 = 4$

$4 \cdot 2 = 8$

$8 \cdot 2 = 16$

$16 \cdot 2 = 32 = 3$

6

12

...

Quicker: successive squaring.

$$2^{13} = 2^8 \cdot 2^4 \cdot 2$$

$$2^4 = (2^2)^2 \qquad 2^8 = (2^4)^2$$

Lot of 2s here.

$3^{13} \mod 29$

$3^8 \cdot 3^4 \cdot 3^1$

$3^4 = (3^2)^2$

$3^8 = (3^4)^2$

$3^1 = 3 \mod 29$

$3^2 = 9$

$(3^2)^2 = 3^4 = 81 = 23 \mod 29$

$3^8 = 7$

$23^2 \equiv (-6)^2 \mod 29.$

$= 36 \equiv 7$

$3^{13} = 3^8 \cdot 3^4 \cdot 3 = 7 \cdot 23 \cdot 3 \mod 29$

$\equiv 7 \cdot 11 \mod 29$

$\equiv 19 \mod 29.$

$a^x \mod n$

write x = sum of powers of 2.

use successive squaring to compute

a^{2^k}.

Exercise 1-(1).

square $5^1 = 5$

square $5^2 = 25$

square $5^4 = 625$

square $5^8 = 762$

square $5^{16} =$.

square $5^{32} =$.

square $5^{64} =$.

square $5^{128} =$.

mod 1979

Need to finish filling in, then use to compute

$5^{143} = 5^{128} \cdot 5^8 \cdot 5^4 \cdot 5^2 \cdot 5^1$

You should use a calculator!

Protip -

$390625/1979 = 197.38\ldots$

so

$390625 \equiv 390625 - 1979 \cdot 197$

$\equiv 762 \mod 1979.$

Scratch.

$(25)^2 = 25 \cdot 25$ $\quad 500 + 125 = 625$

$625 \cdot 625$

$= 375000 + 12500 + 3125$

$= 390625$

$$\begin{array}{r} 197 \\ 1979 \overline{)\,390625} \\ -\,197900 \\ \hline 192725 \\ -\,178110 \\ \hline 14615 \\ 13853 \\ \hline 00762 \end{array}$$

Exercise 2.

$p = 71$ $g = 7$

Trying to get a shared secret.

in this case a number between 0 and 70.

Once you have it, transmit your animal using shift cipher.

E.g. secret is 2

CAT —shift 2→ ECV

ECV —shift 2 back→ CAT

Public: $p = 71$ $g = 7$

Sean

Secret: $a = 3$

I compute

$7^3 \bmod 71$

$343 \bmod 71$

$59 \bmod 71$

$58^3 \bmod 71$

$= 4$

$(7^4)^3 = 7^{12}$

Sunee

$b = 4$

Computes

$7^4 \bmod 71$

$58 \bmod 71$

Public

$X = 59$ $Y = 58$

$59^4 \bmod 71$

$= 4$

$59^4 = (7^3)^4 = 7^{12}$.