Diffie-Hellman Key Exchange

* Code Book Version of this Story

Proven that one-way functions do exist. (easy calculate forward, hard to invert)

$\boxed{\text{Red}} + \boxed{\text{Blue}} \Longrightarrow \boxed{\text{Purple}}$

In any public key scheme, there must be

(1) Some public info (accessible to all)

(2) Some private info

will never find out each other's private key! $\left\{\begin{array}{l}\text{– Alice's Private key (only Alice knows)} \\ \text{– Bob's Private key (only known to Bob)}\end{array}\right.$

Public info key can't compromise either Private key AND

Messages sent between Alice + Bob can't compromise either private key.

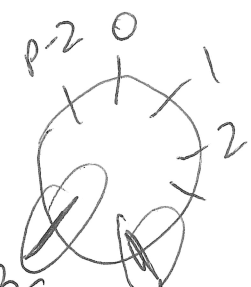
10/28/19 ②

Eve knows $Pu_A = g^{A_E} \bmod p$

$Pu_B = g^{B_E} \bmod p$ $\quad \neq g^{A_E B_E} \bmod p$

$Pu_A \times Pu_B = g^{A_E} \cdot g^{B_E} = \boxed{g^{A_E + B_E}} \bmod p$

$(Pu_A)^{Pu_B} = \left(g^{A_E}\right)^{g^{B_E}} = g^{\boxed{A_E \cdot g^{B_E}}} \neq g^{A_E B_E}$



$g^{A_E} \leftrightarrow A_E$?

$g^{B_E} \leftrightarrow B_E$?

$\phi(13) = 12$

$p = 13$

$g = 2$, $\quad 2^6 \equiv 64 \equiv -1 \bmod 13$

$2^3 \equiv 8 \not\equiv 1 \bmod 13$

$2^4 \equiv 16 \not\equiv 1 \bmod 13$

$p = 13 \qquad g = 2$

$A = 5, \qquad B = 7$

$$\boxed{\begin{array}{c} 2^A \equiv 6 \bmod 13 \\ 2^B \equiv 11 \bmod 13 \\ \text{Eve's Eqn} \end{array}}$$

Alice $\longrightarrow$ Bob $\quad 2^5 \equiv 32 \equiv 6 \bmod 13$

Alice $\longleftarrow$ Bob $\quad 2^7 \equiv 128 \equiv 11 \bmod 13$

Alice computes $\quad 11^5 \equiv (-2)^5 \equiv -32 \equiv -6 \bmod 13 \equiv \boxed{7}$

Bob computes $\quad 6^7 \equiv (36)^3 \cdot 6 \equiv (-3)^3 \cdot 6 \equiv -27 \cdot 6 \equiv -6 \equiv \boxed{7}$

Public Keys

p : large prime $\quad$ g : generator for that prime!

Private Keys

A_E = Alice's Exp $\quad 0 < A_E < p$

B_E = Bob's Exp $\quad 0 < B_E < p$

$$\text{Alice} \xrightarrow{Pu_A = g^{A_E} \bmod p} \text{Bob}$$

$$\text{Alice} \xleftarrow{Pu_B = g^{B_E} \bmod p}$$

Discrete Log Problem (Given these Eve can't figure out A_E, B_E because Disc Log is hard!)

Then, Alice calculates

$$(Pu_B)^{A_E} \bmod p$$

Bob calculate $(Pu_A)^{B_E} \bmod p$

$$(Pu_B)^{A_E} = (g^{B_E})^{A_E} = g^{A_E B_E} \bmod p$$

$$(Pu_A)^{B_E} = (g^{A_E})^{B_E} = g^{A_E B_E} \bmod p$$

This is the shared ~~key~~.