IBE Simplified (CPA-Secure)

Setup

$H_1 : \{0,1\}^* \to G_1$

$H_2 : G_T \to \{0,1\}^n$

$\hat{e} : G_1 \times G_2 \to G_T$

$|G_1| = |G_2| = |G_T| = p$ (prime)

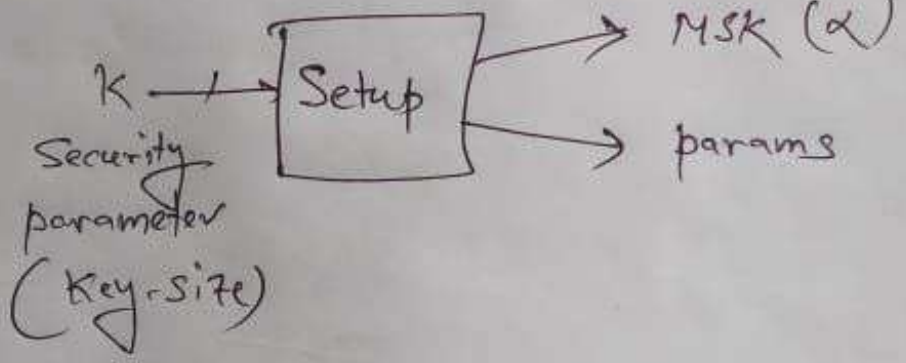
'n': Size of message (no. of bits)

1. $g \xleftarrow{R} G_2$
2. $\alpha \xleftarrow{R} Z_p^*$
3. $g_1 \leftarrow g^\alpha$

outputs

$params = \langle G_1, G_2, G_T, \hat{e}, H_1, H_2, p, g, g_1 \rangle$

$MSK = \langle \alpha \rangle$

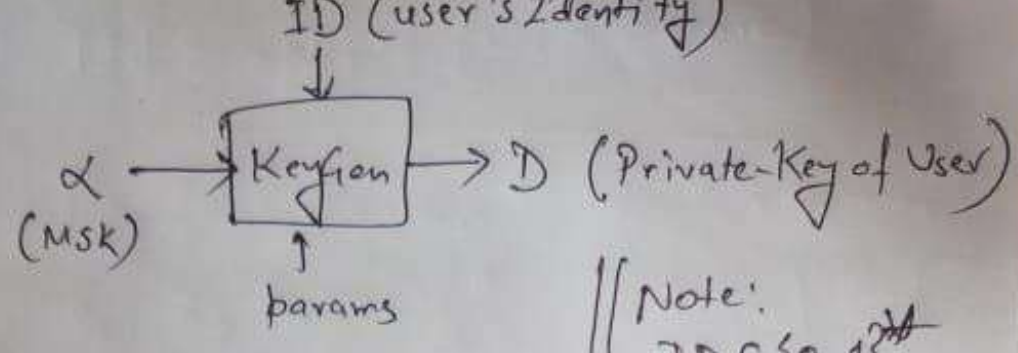


Executed by 'Admin'

MSK given to the KGC

'params' " " All

KeyGen



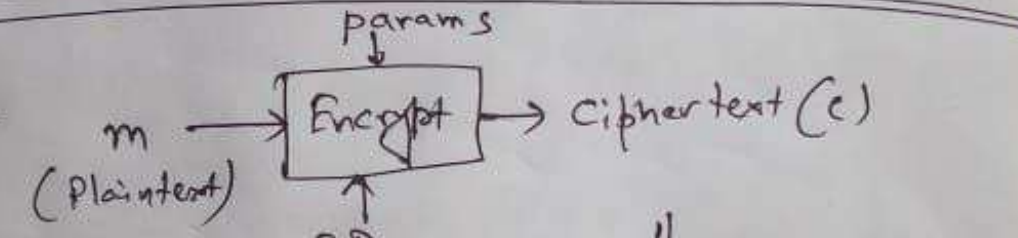
// Note: $ID \in \{0,1\}^{*}$

1. $Q \leftarrow H_1(ID)$
2. $D \leftarrow Q^{\alpha}$

Executed by 'KGC'

Private Key (D) given to the User

Encryption



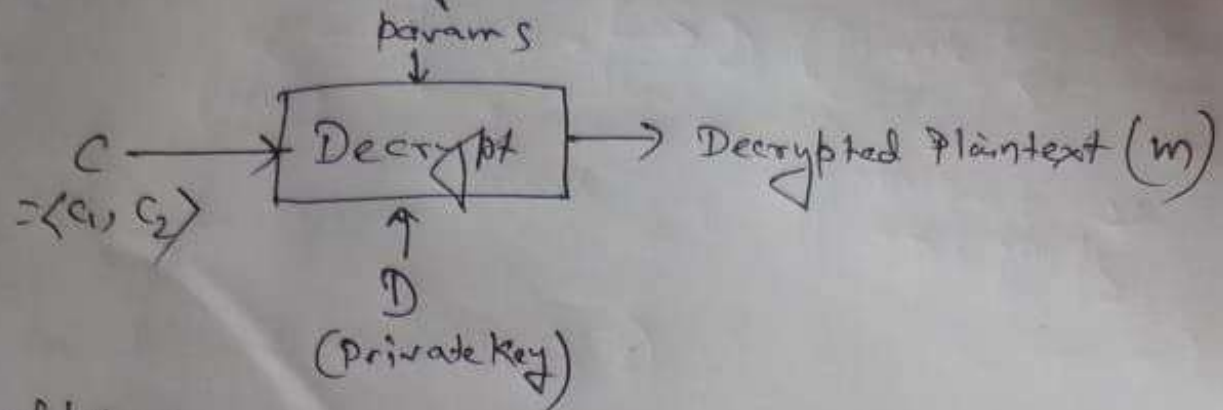
Executed by any 'Sender'

// Note: $m \in \{0,1\}^{n}$

1. $r \xleftarrow{R} \mathbb{Z}_p^{*}$
2. $C_1 \leftarrow g^r$
3. $C_2 \leftarrow m \oplus H_2(\hat{e}(Q, g_1)^r)$

   where $Q = H_1(ID)$
4. $C = \langle C_1, C_2 \rangle$

Decryption



Executed by Receiver

$$C_2 \oplus H_2\left(\hat{e}(D, C_1)\right) \Rightarrow m$$

Correctness Proof:-

$$C_2 \oplus H_2\left(\hat{e}(D, C_1)\right) = C_2 \oplus H_2\left(\hat{e}(Q^{\alpha}, g^{r})\right)$$

$$= C_2 \oplus H_2\left(\hat{e}(Q, g^{\alpha})^{r}\right)$$

$$= C_2 \oplus H_2\left(\hat{e}(Q, g_1)^{r}\right)$$

$$= m \oplus H_2\left(\hat{e}(Q, g_1)^{r}\right) \oplus H_2\left(\hat{e}(Q, g_1)^{r}\right)$$

$$= m$$

Proved

Important Observation:-

Essentially there is a Key Establishment b/t Sender & Receiver.

Sender Calculates $K_1 = e(Q, g_1)^r$

Receiver " $K_2 = e(D, C_1)$

And, $K_1 = K_2$

Now, we calculate the ssn. key by $H_2(K_1)$ or $H_2(K_2)$

And XOR it with the Data (m) or the Ciphertext (C_2)