|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Generar clave** | **CAPTCHA** | **Procesamiento del mensaje** | **Recibir mensaje** | **Descifrar mensaje** | **Desplegar** |
| **Entradas** | * Señal de activación | * Cadena de 5 caracteres: Str(5) | * Clave de 16 bytes: K’(16) * Mensaje de correo | * Correo Cifrado | * Verificación (1,0) | * Correo en claro |
| **Salidas** | * Cadena de 5 caracteres: Str(5) * Clave de 16 bytes: K’(16) | * Señal de envió | * Correo Cifrado | * Verificación (1,0) | * Correo en claro | * - |
| **Descripción** | Se activa el proceso generar clave, este crea una palabra de 5 caracteres(Str(5)), procesa la palabra Str(5) por medio de una función hash obteniendo una palabra de 256 caracteres(K(256)) y recorta esta clave a una palabra de 16 caracteres(K’(16)) | Toma la entrada Str(5) y la convierte en una imagen CAPTCHA, Posteriormente inicia una conexión con el servidor de CAPTCHAS para mandarlo a este. | Cifra el mensaje de correo con la clave K’(16), posteriormente lo firma y genera un timbre para saber que fue creado con este esquema y lo empaqueta para su envió. | El cliente hace una petición al servidor y descarga el mensaje de correo electrónico, lo des empaqueta verifica la firma y el timbrado para saber de quién viene y si está cifrado bajo este esquema | Se hace una petición al servidor de CAPTCHAS, se descargan los CAPTCHAS asociados al correo, ya con el CAPTCHA este se resuelve y se recupera la cadena Str(5), esta se pasa por una función hash y se recupera K(256), esta se corta a K’(16), con esto se descifra el mensaje | Se muestra el correo descifrado en la interface del cliente de correo electrónico |