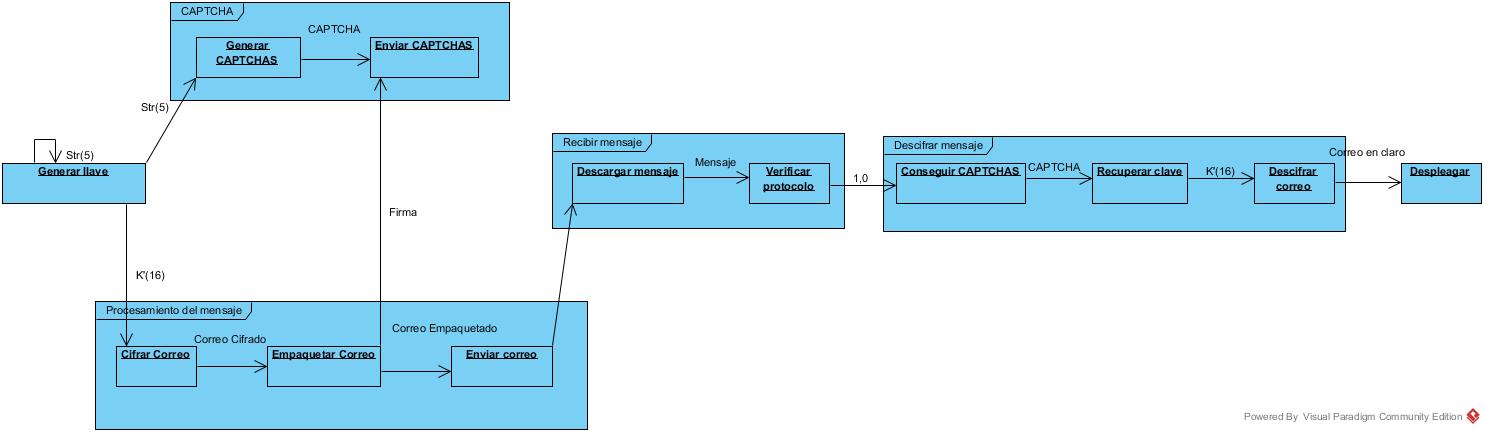
**Diagrama a bloque general del sistema**



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Generar clave** | **Generar 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 |

**Generar clave**



|  |  |  |  |
| --- | --- | --- | --- |
|  | **Generar Str(5)** | **Aplicar Función Hash** | **Recortar Hash K’** |
| **Entradas** | * Llamada a Función | * Cadena de 5 caracteres: Str(5) | * Digesto K(128) |
| **Salidas** | * Cadena de 5 caracteres: Str(5) | * Digesto K(128) | * K’(16) |
| **Descripción** | Toma una función random módulo 67, para formar una palabra con 5 caracteres aleatorios tomados del siguiente conjunto.  Anillo67{-.,+\*[a-z][A-Z]} | Se pasa la cadena Str(5) por una función hash SHA-1 para obtener un digesto único de esta palabra | Se copian a otro string lo primeros 16 caracteres del digesto K(128) para formar la clave K’(16) |

**Cifrar Correo**

|  |  |
| --- | --- |
|  | **Cifrar** |
| **Entrada** | * Clave K’(16) * Mensaje de correo |
| **Salida** | * Correo cifrado |
| **Descripción** | Se cifra el mensaje con un algoritmo de llave simétrica (AES o DES) usando una llave de 16bytes o 128bits |

**Empaquetar Correo**

C:\Users\Administrador\Documents\VPProjects\3Empaquetar Correo.jpg

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Empaquetamiento SMTP** | **Timbrar Correo** | **Firmar Correo** |
| **Entrada** | * Mensaje Cifrado | * Correo Empaqueta | * Correo Timbrado |
| **Salida** | * Correo Empaquetado | * Correo Timbrado | * Correo Correo Timbrado y Firmado * Firma |
| **Descripción** | Se toma el correo y se integra en el formato del correo marcado en el RFC822 | Se timbra el mensaje colocando una marca después del final del mensaje. Para señalar que el correo enviado está cifrado bajo este protocolo | El mensaje se firma a través de ….. para verificar que usuario mando el mensaje. |

**Enviar correo**

C:\Users\Administrador\Documents\VPProjects\4Enviar correo.jpg

|  |  |  |
| --- | --- | --- |
|  | **Abrir conexión SMTP** | **Envió de Correo por SMTP** |
| **Entradas** | * Petición | * Correo empaquetado |
| **Salidas** | * Canal de comunicación | * Confirmación de envió |
| **Descripción** | Se genera una petición para conexión SMTP | Se manda el correo electrónico al servidor por medio del protocolo SMTP |

**Generar CAPTCHA**

C:\Users\Administrador\Documents\VPProjects\5Generar CAPTCHAS.jpg

|  |  |  |
| --- | --- | --- |
|  | **Generar respuesta del CAPTCHA** | **Transformar palabra** |
| **Entradas** | * Cadena de caracteres: Str(5) | * Señal de confirmación |
| **Salidas** | * Señal de confirmación | * Imagen CAPTCHA |
| **Descripción** | Genera un archivo con la respuesta del CAPTCHA | Convierte el Str(5) en una imagen distorsionada que llamaremos CAPTCHA |

**Enviar CAPTCHAS (Usuario existente)**

C:\Users\Administrador\Documents\VPProjects\6Enviar_CAPTCHA.jpg

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Abrir conexión** | **Verificar Usuario** | **Mandar CAPTCHA** | **Registrar en base de datos** | **Cerrar Conexión** |
| **Entradas** | * CAPTCHAS | * Datos de Usuario | * Verificación de usuario | * Datos de usuario * CAPTCHA | * Verificación |
| **Salidas** | * Datos de usuario | * Verificación de usuario | * CAPTCHA | * Verificación |  |
| **Descripción** | Se genera una petición para poder entablar una conexión con el servidor de CAPTCHAS | Se verifica la existencia del usuario en el servidor, si existe se le da acceso | Ya verificado el usuario se manda el CAPTCHA al servidor | Se registran los datos del CAPTCHA en la base de datos y se envía una verificación | Se cierra la conexión y se guardan los datos |

**Enviar CAPTCHAS (Usuario inexistente)**

**C:\Users\Administrador\Documents\VPProjects\7bisEnviar CAPTCHAS usuario inexistente.jpg**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Abrir conexión** | **Registrar usuario en Base de Datos** | **Verificar Usuario** | **Mandar CAPTCHA** | **Registrar en base de datos** | **Cerrar Conexión** |
| **Entradas** | * CAPTCHAS | * Datos de usuario | * Verificación de registro | * Verificación de usuario | * Datos de usuario * CAPTCHA | * Verificación |
| **Salidas** | * Datos de usuario | * Verificación de registro | * Verificación de usuario | * CAPTCHA | * Verificación |  |
| **Descripción** | Se genera una petición para poder entablar una conexión con el servidor de CAPTCHAS | Se da de alta al usuario en la base de datos | se le da acceso al usuario | Ya verificado el usuario se manda el CAPTCHA al servidor | Se registran los datos del CAPTCHA en la base de datos y se envía una verificación | Se cierra la conexión y se guardan los datos |

**Descargar mensaje**C:\Users\Administrador\Documents\VPProjects\8Descargar mensaje.jpg

|  |  |  |
| --- | --- | --- |
|  | **Abrir conexión al servidor de correo** | **Descargar mensaje por IMAP o POP3** |
| **Entradas** | * Señal de activación | * Confirmación |
| **Salidas** | * Confirmación | * Correo electrónico |
| **Descripción** | El receptor se conecta al servidor de correo electrónico e inicia la sesión | Descarga del servidor de correo electrónico todos los mensajes que aún no se hallan descargado. |

**Verificar protocolo (con protocolo valido)**

C:\Users\Administrador\Documents\VPProjects\9Verificar_CAPTCHA.jpg

|  |  |  |
| --- | --- | --- |
|  | **Abrir mensaje** | **Verificar mensaje** |
| **Entradas** | * Correo electrónico | * mensaje |
| **Salidas** | * Mensaje | * verificación |
| **Descripción** | Se toma el mensaje descargado del servidor y se des empaqueta para dejar solo el texto del mensaje | Se verifica que el mensaje tenga la bandera correspondiente a que está cifrado con este esquema |

**Verificar protocolo (con protocolo invalido)**

|  |  |  |
| --- | --- | --- |
|  | **Abrir mensaje** | **Verificar mensaje** |
| **Entradas** | * Correo electrónico | * mensaje |
| **Salidas** | * Mensaje | * verificación |
| **Descripción** | Se toma el mensaje descargado del servidor y se des empaqueta para dejar solo el texto del mensaje | Si la verificación es negativa se manda directamente al bloque de Despliegue |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Abrir Conexión** | **Validar Usuario** | **Accesar a cuenta** | **Verificar existencia de CAPTCHA** | **Enviar CAPTCHA** | **Cerrar Conexion** |
| **Entradas** | * Confirmacion | * Datos usuario | * Contraseña | * Petición de CAPTCHAS | * Confirmacion | * Peticion |
| **Salidas** | * verificacion | * Contraseña | * confirmacion | * confirmacion | * CAPTCHA | * Confirmacion |
| **Descripción** | Se abre una conexión con el servidor de CAPTCHAS | Se verifica que el usuario este dado de alta en el servidor mandándole una petición a la base de datos, si el usuario existe se accesa | Si esta dado de alta en el servidor se manda la contraseña para que pueda tener acceso a los CAPTCHAS de su cuenta | Se verifica que los CAPTCHAS que están ligados al mensaje que realizo la petición existan | Si existen estos CAPTCHAS son enviados de regreso al mensaje | Ya enviados los CAPTCHAS se cierra la conexión con el servidor |

**Conseguir CAPTCHAS (Usuario existente)**C:\Users\Administrador\Documents\VPProjects\10Conseguir_captcha.jpg

**Recuperar clave**C:\Users\Administrador\Documents\VPProjects\10Recuperar clave.jpg

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Resolver CAPTCHA** | **Aplicar Función Hash** | **Recortar llave** |
| **Entradas** | * CAPTCHA | * Cadena de 5 caracteres: Str(5) | * Digesto K(128) |
| **Salidas** | * Str(5) | * Digesto K(128) | * K’(16) |
| **Descripción** | Se despliega el CAPTCHA para que el usuario pueda resolverlo | Se pasa la cadena Str(5) por una función hash SHA-1 para obtener un digesto único de esta palabra | Se copian a otro string lo primeros 16 caracteres del digesto K(128) para formar la clave K’(16) |

**Descifrar correo**

|  |  |
| --- | --- |
|  | **Descifrar** |
| **Entrada** | * Clave K’(16) * Mensaje de correo |
| **Salida** | * Correo descifrado |
| **Descripción** | Se descifra el mensaje con un algoritmo de llave simétrica (AES o DES) usando una llave de 16bytes o 128bits |