Criptografía: Aspectos Teóricos y Prácticos — Laboratorio 2: Terminar la implementación de RSA

En este laboratorio terminarán de implementar las especificaciones oficiales de RSA:

`http://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf`

En esta segunda parte se implementarán todas las funciones de encriptar y las funciones relacionadas con las firmas digitales. Se entregará esta primera parte el **viernes 13 de junio**. Lo entregarán por EVA y **lo harán en equipos de por lo menos dos integrantes**.

1. **RSAES-OAEP-ENCRYPT** Implementar la función descrita en la página 18 y verificar que funcione con los vectores de prueba en el archivo `oaep-vect.txt`.
2. **RSAES-OAEP-DECRYPT** Implementar la función descrita en la página 21 y verificar que funcione con los vectores de prueba en el archivo `oaep-vect.txt`.
3. **EMSA-PSS-ENCODE y EMSA-PSS-VERIFY** Implementar las funciónes descritas en las páginas 37 y 38.
4. **RSASP1 y RSAVP1** Implementar estas funciones descritas en las páginas 13 y 14. Observar que son casi idénticas a las funciones **RSAEP** y **RSADP**.
5. **RSASSA-PSS-SIGN** Implementar la función descrita en la página 28 de las especificaciones. Verificar que funcione con los datos en el archivo `pss-int.txt`.
6. **RSASSA-PSS-VERIFY** Implementar la función descrita en la página 30 de las especificaciones Verificar que funcione con los datos en el archivo `pss-vect.txt`.
7. En los ejercicios, cuando pido que verifiquen que una función funcione para ciertos archivos, pido que tengan una función llamado, por ejemplo, `test-rsaes-oaep-encrypt()` que carga el archivo correspondiente y después imprime, para cada componente del vector, si tu implementación devuelve el resultado predicho por el archivo o no:

   ```
   First test passed...
   Second test passed...
   ```

   y etc.