UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE CIENCIAS
ESCUELA DE COMPUTACION

CRIPTOGRAFIA

CODIGO: 23H1
TIPO: ELECTIVA
REQUISITOS: 2309-2308.
CREDITOS: 5

PROGRAMA

1. **Nociones Fundamentales.**
   Criptografiá. Seguridad de Datos. Sistemas Criptográficos. Privacidad y Autenticidad. Criptosistemas Simétricos y Asimétricos. Criptosistemas con Claves Públicas. Firmas Digitales.

2. **Algoritmos Criptograficos.**
   Transposición. Sustitución Simple. Sustitución Homofónica. Sustitución Polialfabética.

3. **El Algoritmo ASA.**
   Congruencias. Aritmética Modular. Cifrados Exponenciales. Descripción del algoritmo Asa.

4. **El Algoritmo DES.**
   Cifrados por productos. Descripción del algoritmo DES. Generación de las Claves Internas. Función de desciframiento.

5. **Tecnicas Criptograficas.**
   Cifrados en bloques y continuas. Cifrados continuos sincrónicos. Cifrados continuos autosincrónicos. Cifrados en bloque con encadenamiento.

6. **Manejo de Claves.**
   Sistemas convencionales. Control centralizado. Control distribuido. Control jerárquico. Sistemas públicos. Comparación entre los sitemas convencionales u públicos.

7. **Control del Flujo de la Información.**
   Modelo reticular. Mecanismos de control de flujo. Mecanismos a tiempo de ejecución. mecanismos a tiempo de compilación. Verificación de programas. El sistemas ACCat Guard en la red ARPANET.

REV/1991