Nombre:

Ejercicios de Técnicas clásicas de cifrado

- 1. Mencione los tres criterios para clasificar los sistemas criptográficos.
- 2. Defina sustitución y transposición.
- 3. ¿Cuál es la condición necesaria para que un algoritmo afín con decimación tenga proceso de descifrado?
- 4. Matemáticamente, ¿por qué el cifrado de Hill es un algoritmo que trabaja en bloques?
- 5. ¿Por qué el cifrado de Vernam utiliza la operación lógica XOR?

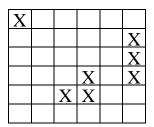
En los <u>ejercicios del 6 al 10 cifre</u> el mensaje en claro mediante el primer algoritmo que se indica, y el criptograma resultante cífrelo con el segundo algoritmo. Trabaje en módulo 27.

- 6.- Mediante el algoritmo de Hill con clave K = ANTIVIRUS y transposición doble. Mcla = EL TIBURON AZUL
- 7.- Por medio de Vigenère con K = INMOLARSE y transposición simple. Utilice la tabla de Vigenère dada en clase (n=37). Mcla = UN BELLO BOSQUE ABANDONADO
- 8.- Con el algoritmo afín de sustitución por desplazamiento variable con K = BUSQUEDA y transposición por columnas con Nc = 6. Mcla = ¿DONDE ESTARAS ESTRELLA GEMELA?
- 9.- Mediante el algoritmo afín con decimación a = 14 y desplazamiento b = 9, y transposición por renglones con clave K = BALON. Mcla = VIAJE A LAS ESTRELLAS
- 10.- Haciendo uso del algoritmo Vernam con $K = \#0_s^{[}$ y transposición por grupos con permutación $P_M = 634152$. Mcla = ¿Estás ahí?
- 11.- Por medio del disco de Alberti con coincidencia inicial A #, n = 1 a la derecha cada 3 sustituciones, y transposición inversa. Mcla = IGUAL QUE LA NIEBLA ANTE EL SOL, LA IGNORANCIA SE DISIPA ANTE EL CONOCIMIENTO (Para realizar el ejercicio de Alberti utilice el disco construido en clase)

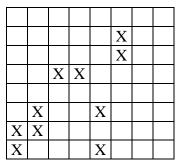
En los <u>ejercicios del 12 al 20 descifre</u> el criptograma dado, considerando que dicho criptograma se obtuvo empleando dos algoritmos criptográficos, el primer algoritmo utilizado es el primero que se indica, y enseguida se menciona el segundo algoritmo empleado. Trabaje en módulo 26.

12.- El Cripto = icnof fnade uvsgv mjair fvpbn lvwal se obtuvo mediante transposición por grupos con P_M = 361524 y cifrado afín con decimación a = 5 y desplazamiento variable con k = AVION.

- 13.- El Cripto = rlriax emedap mljscq xkvstw oigweh dgessw se obtuvo por Vigenère con K = ASTEROIDE y transposición por columnas con K = EXTRAS.
- 14.- El Cripto = FVMYA TWRBV LUHKE MAZJK HXKHL CQCEU se obtuvo mediante cilindro de Bazeries (usado en clase con el alfabeto básico en español y Transposición doble.
- 15.- El Cripto = CBZZLZ SOLSLL INZAIC ORLZUR SIEOOE ZEZZNN se obtuvo mediante máscaras rotativas (con la máscara aquí mostrada) y transposición simple.



16.-El Cripto = zba"bcd; e~gfgk:@ huxyfñwi jkp;vhli wminyvnñ o;mcor^p imqqrvis "tuv~wb/ se obtuvo mediante el disco de Alberti (disco construido) con K=(A%,2,2d) y máscaras rotativas (con la máscara aquí mostrada)



- 17.- El Cripto = POALYT LAESEO IMBGRM RANIRN LRQERL NALULO LETVAB SRAAPS EEEESE UUAUML SVTREE se obtuvo mediante transposición por series (s_1 =serie de fibonacci, s_2 =números primos, s_3 =números pares, s_4 =números naturales) y transposición por columnas con N_C =6.
- 18.- El Cripto = ZPQDD QSWSL WIVTA OZUFD PDSLH NNRZJ JPEXS NWQHD se obtuvo mediante cilindro de Bazeries (usado en clase con el alfabeto básico en español y Transposición simple.
- 19.- El Cripto = HCTBBQ se obtuvo mediante el algoritmo de Hill con k=CONVERSAR (n=27) y Afín por desplazamiento puro variable con k=CORUÑA.
- 20.- El Cripto = #1/D1 % $6+\ddot{E}g$ % $6*\dot{E}e$ SPACE $0*\dot{D}$ "a* \dot{E} se obtuvo mediante el algoritmo POLYBIOS y VERNAM con k= arn \dot{E} \$