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 siguientes ejercicios **cifre** 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 , n=27 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 , n=27 y transposición por columnas con Nc = 6. Mcla = ¿DONDE ESTARAS ESTRELLA GEMELA?

9.- Mediante el algoritmo afín – afin, con n=27 , 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?

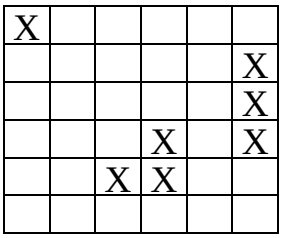
En los siguientes ejercicios **descifre** el criptograma dado, considerando que dicho criptograma se obtuvo empleando dos algoritmos criptográficos, el primer algoritmo utilizado es el primero que se indica, y enseguida se menciona el segundo algoritmo empleado. Trabaje en módulo 26.

11.- 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.

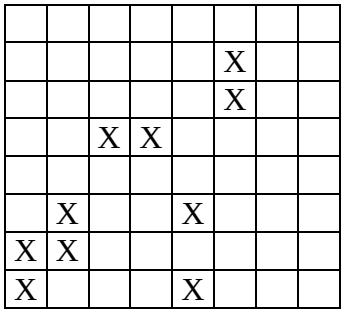
12.- El Cripto = rlriax emedap mljscq xkvstw oigweh dgessw se obtuvo por Vigenère con K = ASTEROIDE y transposición por columnas con K = EXTRAS.

13.- 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.

14.- El Cripto = CBZZLZ SOLSLL INZAIC ORLZUR SIEOOE ZEZZNN se obtuvo mediante máscaras rotativas (con la máscara aquí mostrada) y transposición simple.



15.- 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)



16.- 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.

17.- 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.

18.- El Cripto = HCTBBQ se obtuvo mediante el algoritmo de Hill con k=CONVERSAR (n=27) y Afín por desplazamiento puro variable con k=CORUÑA.

19.- El Cripto = #1/Ð1 %6+Ëg %6*Êe SPACE 0*Ð` ”a*Ê se obtuvo mediante el algoritmo POLYBIOS y VERNAM con k= arnÉ$

20.- Descifre el mensaje oculto en el siguiente texto:

ESTA MAÑANA HICE MI GRAN TAREA DE REPOSTERÍA Y PIENSO FUE LA ACTIVIDAD QUE MÁS ENTRETENIDA TUVE EN LA SEMANA Y QUE ME PARECIÓ MÁS DIVERTIDA