Actividad: Cifrados de Vigenère y Hill

**Objetivos**

* Con esta actividad vas a conseguir entender cómo se cifra y se descifra con el algoritmo monográmico polialfabético de Vigenère y con el algoritmo poligrámico monoalfabético de Hill, los sistemas de cifra clásica más importantes, en módulo 27 (mayúsculas español), 26 (mayúsculas inglés) y 191 (subconjunto con un número primo de caracteres imprimibles del ASCII extendido).
* Vas a comprobar que la cifra de Vigenère puede criptoanalizarse mediante el uso de las estadísticas y la redundancia del lenguaje, usando el método de Kasiski.
* Vas a comprobar que la cifra con matrices de Hill puede criptoanalizarse mediante el uso de propiedades matemáticas, usando el método de Gauss-Jordan.

**Descripción**

Se usará el *software* de prácticas Criptoclásicos v2.1 para todas las operaciones.

<http://www.criptored.upm.es/software/sw_m001c.htm>

**Enunciado de la práctica**

1. Cifrado y descifrado de Vigenère
   1. Con el algoritmo de Vigenère en mod 27, cifra el siguiente texto M con la clave K.

M = El final del verano llegó y tú partirás

K = Dúo Dinámico

**Entrega en el informe solamente el criptograma en bloques de 5 letras.**

* 1. Con el algoritmo de Vigenère en mod 191, descifra el criptograma C sabiendo que la clave era: Monólogo del replicante Roy Batty

C = ¥ÝÕXá ×ÙâÒÇ ÚäÅâÜ ÝÇÖÜæ ÓÅàç´ ÎâÖê± ÓßàÌ× Ù|¤ØÌ ÔÅáÙÉ ØÅàØÒ ½ÚÙ®Á æàZ¿Ï Ù\_MÒË ½ÕÍ\_ß r·ÐÞË ÓáâÖ² çç´m¶ ÕêµÚÙ TÝÓÔÚ ÄÓÞÔÙ áÔÌÃÄ ÐØÖ´Ï Ü¦ÌÔÃ í±àáT ÏÓºÏÑ ÒÓVÙâ ÐÚp´Ü ×ÓÄÓë °Óàâå ±ÜábÞ áËÞÈÖ ÏÖÖQÙ ÍÐÅÙç Í¶Ûè° lÖâå» ÚOZÝ× ÓÏÖÉÙ ÝÅÛ×Ý ØÉÎ¡© ÄÖç³Á ×Øå»à Öey

**Entrega en el informe solamente el texto en claro encontrado, incluyendo los espacios en blanco de separación de palabras.**

1. Cifrado y descifrado de Hill
   1. Con la clave digrámica indicada cifra en mod 26 (inglés) el texto Merry Christmas.

18 9

15 23

**Entrega en el informe solamente el criptograma en bloques de 2 letras.**

* 1. Con la clave trigrámica indicada, descifra en mod 27 el criptograma C.

5 7 12

1 21 21

5 2 1

C = QNQ WHO RES RAU QXB IBV ÑDV GYS ÑNZ JEB LFJ IKJ

**Entrega en el informe solamente el texto en claro encontrado, incluyendo los espacios en blanco de separación de palabras.**

1. Criptoanálisis de Vigenère y Hill
   1. Criptoanaliza el criptograma que se indica cifrado con Vigenère mod 27.

C = EWZYI NEMEJ IZMLJ ÑAAVX AWJWL JAUWN LWLHX GAAMX FQUVI WATAM XÑPSM RZMDT ZÑPET MCZSV BWASE IOKNB WWLHM WASUB LQQSG IZMDT JWZKI KQPSW BLSNZ TÑIVÑ WWAEÑ RBCFW TZILE TYCWM NEWFW XOPWE GEVHO BRPWM XHWTT MPIFN XMIKT JLLWL EHMÑT LQUFI FXZWV ÑWSJÑ BAZSM BHIAF JLZMT GPPLB FWKNX MPPHG MAONU BAZSL XOCWE NLMFM XJBAW IJMYT NEDHX MIILK ÑAXKI UWJDX KQMWM NWAEX FLZAT MJWZÑ UEMLX OEAMI GQUUT EWSNS JQJDB VWGSÑ GOCII GEMFW INCWR IHILA ÑXPWM XAAUL BPWFI AWJKB TJITT LYIVI FWAVX WLAIT ZEUSM RDCTB XÑIFJ IOMAW IASEX LEBHB GAAMB FWJDX WAAWL XHMBX FMSSL FWAXB XHGUI GYPLI WAJAI ZÑIXB TZMJÑ XAUÑT GAKWL MAXNX WWSSE BPMKT NQZSW XPWVT MHILX JLKSM RZMMI WLADI MMIAM XO

**Entrega en el informe solamente la clave encontrada y las 3 primeras palabras del texto claro encontrado.**

* 1. Criptoanaliza el criptograma C si se sabe que se ha cifrado con Hill mod 191 en bloques de 4 letras y que el texto en claro comienza por:

Dime de qué presumes

C = «BÝ. 0Çß$ nãÏ¢ òzd¦ 0È¯R ìàqÕ 0Çß$ UËË´ àTµ8

**Entrega en el informe la matriz clave encontrada y el texto en claro completo, añadiendo los espacios en blanco para separar palabras.**

**Rúbrica:**

|  |  |  |  |
| --- | --- | --- | --- |
| Título de la actividad | Descripción | Puntuación máxima  (puntos) | Peso  % |
| Criterio 1 | Los resultados entregados del apartado 1 son correctos | 3 | 30% |
| Criterio 2 | Los resultados entregados del apartado 2 son correctos | 3 | 30% |
| Criterio 3 | Los resultados entregados del apartado 3 son correctos | 4 | 40% |
|  |  | **10** | **100 %** |

**Extensión:** 1 página (incluir solamente las respuestas, no las capturas de pantalla).