

**Universidad de Buenos Aires**

**Facultad de Ingeniería**

**Departamento de Informática**

***Organización de Datos (75.06)***

**Voto Electrónico**

**Vigenere y Kasiski**

Cuatrimestre y año: 2do Cuatrimestre 2011

Docente a cargo del TP:Nicolás Pablo Fernández Theillet

Grupo: Lamas

Fecha de Entrega: 2011-11-03

Integrantes:

|  |  |  |
| --- | --- | --- |
| ***Padrón*** | ***Nombre*** | ***Email*** |
| 91187 | Gonzalez Durand, Juan Manuel | jmanuel.gonzalez.durand@gmail.com |
| 90762 | Ostrowsky, Gabriel | gaby.ostro@gmail.com |
| 90728 | Schenkelman, Damián | damian.schenkelman@gmail.com |
| 91045 | Torrado, Alejandro | aletorrado@gmail.com |
| 90884 | Zamudio, Gonzalo | ahogadosderazon@gmail.com |

Cifrado de Vigenere

A continuación se detalla la implementación del cifrado de Vigenere utilizada para el trabajo práctico y el uso de la misma para encriptar y desencriptar reportes.

## Encriptación de Reportes

1. Cuando se quiere guardar un reporte en disco, se pide una clave al usuario. La misma puede tener la cantidad de caracteres que el usuario desee, siempre que estos sean imprimibles. Para este ejemplo supongamos que la clave es **MICLAVE**.
2. Una vez que el usuario ingresa su clave, se encripta el reporte. Para mantener la estructura del reporte y tener la posibilidad de hacer el ataque de Kasiski, solo se encriptan las letras. Por ejemplo, si tenemos el siguiente reporte, solo los caracteres resaltados se encriptaran:

|  |  |
| --- | --- |
| **Reporte sin encriptar** | **Reporte encriptado** |
| DISTRITO: YUMA  GANADOR DE ELECCION: GOBERNADOR PROV NRO 107, 10-12-2011  LISTA: LISTA 3 VOTOS: 18  GANADOR DE ELECCION: INTENDENTE DE YUMA, 15-11-2011  LISTA: LISTA 3 VOTOS: 13  GANADOR DE ELECCION: PRESIDENTE NRO 6 FECHA: 12-11-2011  LISTA: LISTA 2 VOTOS: 20 | PQUERDXA: GWXA  BEZIFZR YI QTGNCDSZ: OQMEMRMLQC PMSH VTZ 107, 10-12-2011  LDWFI: NTSOE 3 HWVZS: 18  BEZIFZR YI QTGNCDSZ: QPEEIHQVVP DZ CGUC, 15-11-2011  WINXM: TKDTV 3 ZABQD: 13  GVRMLQC DZ IXMENIJR: BZGDIYIZBG YRJ 6 JQKJL: 12-11-2011  LDWFI: NTSOE 2 HWVZS: 20 |

Los reportes se guardan en el directorio **Files/Reports**.

## Cifrado de Vigenere

Para el cifrado, utilizamos el siguiente algoritmo:

1. Apareamos cada letra del mensaje (mi) con una letra de la clave (ki).
2. Obtenemos el símbolo relacionado del criptograma ci de la forma:

crypted = ((message[i] + key[j]) % 26) + 'A';

En el caso de la clave **MICLAVE**, y la palabra **DISTRITO** las operaciones y el resultado serían:

