



Taller 02

Gestión de Seguridad Informática

Grupos de 2 integrantes

Profesor: Patricio Collao Caiconte

Fecha:

- Sesión 1: miércoles, 28 de octubre de 2020 (trabajo)
- Sesión 2: lunes, 02 de noviembre de 2020 (trabajo)
- Sesión 3: miércoles, 04 de noviembre de 2020 (presentación de resultados y pruebas entre grupos)

Nombre del Proyecto: Implementación de cifrador polialfabético

Tipo del Proyecto:

- ☐ Estudio de Caso
- ☐ Desarrollo de Proyecto
- ☒ Aprendizaje Basado en Problemas
- ☒ Desarrollo de Actividades para el Trabajo Colaborativo/equipo
- ☒ Uso de Tecnología Moderna

OBJETIVO	DESCRIPCIÓN	METAS
Desarrollar competencias de autoaprendizaje, trabajo en equipo en los alumnos de la asignatura.	Resolver problemas a través de la simulación del algoritmo criptográfico de llave secreta.	Capacidad de análisis y entendimiento de una técnica de cifrado y descifrado. Capacidad de autoaprendizaje. Capacidad de programar en un lenguaje de alto nivel.

ACTIVIDADES: (3)

1. Entrega del enunciado en primera sesión

Utilizando el algoritmo Cifra polialfabética:

Ejemplo parcial con alfabeto ingles

- Secuencia: C1, C2, C2, C1, C2

Letras texto abierto	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
C1 (k=5)	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
C2 (k=19)	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r

2. Implementar con interfaz gráfica, utilizando HTML, CSS y JS, el cifrador polialfabético, en las cuales las claves y la secuencia sean ingresadas por el usuario.
3. En la sesión 3:
 - Entregar:
 - i. Código fuente
 - ii. Build (si lo hay)
 - iii. Video (10 min máximo) explicando principales partes y etapas en el código fuente.
 - Presentación de lo realizado (5 min por grupo) y emitir en secreto un mensaje cifrado de 20 a 30 letras, indicando las claves usadas.
 - Pruebas de comunicación entre grupos

CONSIDERACIONES:

Implementación:

- 1) Usar alfabeto español de 27 letras
- 2) La secuencia puede tener entre 2 y 6 elementos, siempre combinando C1 y C2. Ej C1C1C2C1C2C1
- 3) C1 y C2 pueden tener valores entre 1 y 26
- 4) El texto claro y cifrado deben estar en mayúsculas
- 5) En el texto claro se debe usar la letra X donde haya espacios. Texto claro "HOLA MUNDO" (interfaz usuario) -> "HOLAXMUNDO" (interno)
- 6) No se debe usar la letra X en el texto claro original.

Video:

- 1) Puede estar separado en hasta 3 partes

CONCLUSIONES:

Al término del trabajo el alumno deberá ser capaz de implementar el algoritmo de cifra polialfabética.