IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT

… en 4º ESO

liylmnp

v2 4º ESO Matemáticas para la toma de decis...

Copiar enlace de invitación

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

ORDEN ECD/1172/2022, de 2 de agosto, por la que se aprueban el currículo y las características de la evaluación de la Educación Secundaria Obligatoria y se autoriza su aplicación en los centros docentes de la Comunidad de Aragón.

Capítulo II Ordenación del currículo.

Artículo 11. Distribución de las materias en la Educación Secundaria Obligatoria.

5. En cuarto curso de la Educación Secundaria Obligatoria, el alumnado cursará:

c) De entre estas materias, el alumnado cursará una de ellas:

- **Artes Escénicas y Danza.**
- **Cultura y Patrimonio de Aragón.**
- **Cultura Científica.**
- **Cultura Clásica II.**
- **Filosofía.**
- **Lenguas Propias de Aragón: Aragonés o Catalán**
- **Matemáticas para la toma de decisiones.**
- **Oratoria y Escritura.**

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

4º ESO

MATEMÁTICAS PARA LA TOMA DE DECISIONES

Los saberes se han organizado en tres grandes bloques:

- **Aritmética modular y criptografía.**
- **Teoría de grafos.**
- **Teoría de juegos.**

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

4º ESO
MATEMÁTICAS PARA LA TOMA DE DECISIONES
Aritmética modular y criptografía.

"El bloque dedicado a la aritmética modular y la criptografía, a partir de conocimientos previos de los estudiantes, presenta algunos de los fundamentos de la tecnología digital. La aritmética básica es un campo en el surgen de manera natural un buen número de conjeturas y propiedades que estudiar con ayuda de **medios informáticos**. Además, la aritmética modular se encuentra en la base del tratamiento informático de datos y la criptografía resulta indispensable en un mundo en el que la identidad digital es casi equivalente a la identidad real de una persona.

"El **pensamiento computacional, el diseño y aplicación de algoritmos**, así como su análisis deben estar presentes de manera sustancial a los largo de los tres bloques. El **uso de herramientas informáticas** debe ser constante para representar objetos y situaciones, formular conjeturas y ponerlas a prueba y para encontrar soluciones a problemas de forma efectiva y constructiva."

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

4º ESO
MATEMÁTICAS PARA LA TOMA DE DECISIONES
Aritmética modular y criptografía.

COMPETENCIAS ESPECÍFICAS:

CE.MTD.1. Reconocer la importancia de la aritmética modular en un contexto tecnológico y digital, comprendiendo la necesidad y los fundamentos básicos de algoritmos de codificación sencillos y siendo capaz de aplicarlos de forma efectiva a situaciones concretas.

CE.MTD.4. Emplear herramientas de cálculo simbólico u otras herramientas digitales para representar resultados y procedimientos, explorar, conjeturar y comprobar propiedades, y resolver problemas, desarrollando e implementando algoritmos matemáticos sencillos.

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

4º ESO
MATEMÁTICAS PARA LA TOMA DE DECISIONES
Aritmética modular y criptografía.

CRITERIOS DE EVALUACIÓN:

CE.MTD.1. En los bloques dedicados a la aritmética, el énfasis se pone en **aspectos conceptuales más que en los operativos**. Los cálculos se realizan con **calculadora** o, preferiblemente con **ordenador**, de modo que lo importante es saber qué hacer y cómo hacerlo. En la resolución de ecuaciones y de congruencias es muy importante el estudio de la existencia de solución. En el bloque de criptografía, de nuevo, se hace especial énfasis en conocer los fundamentos de los algoritmos y sus debilidades.

1.1. Aplicar el **algoritmo de Euclides** para calcular el m.c.d. de dos números y para obtener la expresión de la identidad de Bezout.
1.2. Resolver **ecuaciones diofánticas lineales** en una y dos variables, estudiando previamente la existencia de solución.
1.3. Poseer los fundamentos necesarios para trabajar **módulo un entero m**, sabiendo las diferentes propiedades que surgen según m sea primo o no.
1.4. Resolver de forma constructiva **sistemas de congruencias lineales** con una incógnita, estudiando previamente la existencia de solución.
1.5. Conocer y determinar **unidades y divisores de cero en Z/mZ** para cualquier m.
1.6. Aplicar el **pequeño teorema de Fermat** para estudiar la primalidad de un entero dado.
1.7. Conocer, idear y aplicar algoritmos de **cifrado de sustitución y polialfabéticos sencillos**, entendiendo sus vulnerabilidades.
1.8. Conocer los fundamentos y vulnerabilidades del **algoritmo RSA**, aplicándolo en casos sencillos.

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

4º ESO
MATEMÁTICAS PARA LA TOMA DE DECISIONES
Aritmética modular y criptografía.

CRITERIOS DE EVALUACIÓN:

CE.MTD.4. La propia naturaleza de los contenidos abordados en esta materia implica una **fuerte carga computacional**. Esto conlleva, por una parte, la necesidad de utilizar de forma esencial y significativa **herramientas informáticas** y, por otra, la capacidad de idear e **interpretar algoritmos**. A este respecto, no es necesario conocer ningún lenguaje de programación, pero sí manejar de forma operativa las ideas de bucles y condicionales. En todo caso, el trabajo con esta competencia estará siempre centrado y orientado hacia los distintos saberes básicos que conforman la materia.

4.1. Formular conjeturas acerca de propiedades de los **números enteros** y estudiar su posible veracidad o falsedad de forma computacional.
4.2. Utilizar herramientas informáticas para **explorar propiedades de grafos**.
4.3. Diseñar algoritmos propios para resolver **problemas aritméticos en Z y en Z/mZ.**
4.4. Expresar en **pseudocódigo los algoritmos aritméticos** sencillos diseñados.
4.5. Analizar y comprender el funcionamiento de **algoritmos sencillos** expresados en pseudocódigo en contextos de aritmética, teoría de grafos y teoría de juegos.

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

4º ESO
MATEMÁTICAS PARA LA TOMA DE DECISIONES
Aritmética modular y criptografía.

SABERES BÁSICOS:

A.1. Aritmética en Z:	**A.2. Aritmética modular:**	**A.3. El conjunto Z/mZ:**	**A.4. Criptografía:**
- La relación de divisibilidad. -Máximo común divisor y mínimo común múltiplo. - Algoritmo de Euclides. Identidad de Bezout. - Números primos. El teorema fundamental de la aritmética. - Ecuaciones diofánticas lineales. Resolución completa de los casos con una y dos variables.	- La relación de congruencia módulo un entero m. Propiedades. - Inversos multiplicativos. Existencia y cálculo. - Resolución de congruencias lineales con una incógnita. - Resolución de sistemas de congruencias lineales con una incógnita. El teorema chino de los restos.	- El conjunto de clases módulo m. - Unidades y divisores de cero. La función phi de Euler. - Orden de un elemento. - El pequeño teorema de Fermat y el teorema de Euler.	- Esteganografía y criptografía. Origen, utilidad y aplicaciones. - Cifrados de sustitución y polialfabéticos. - Cifrados simétricos y asimétricos. - El algoritmo RSA.

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

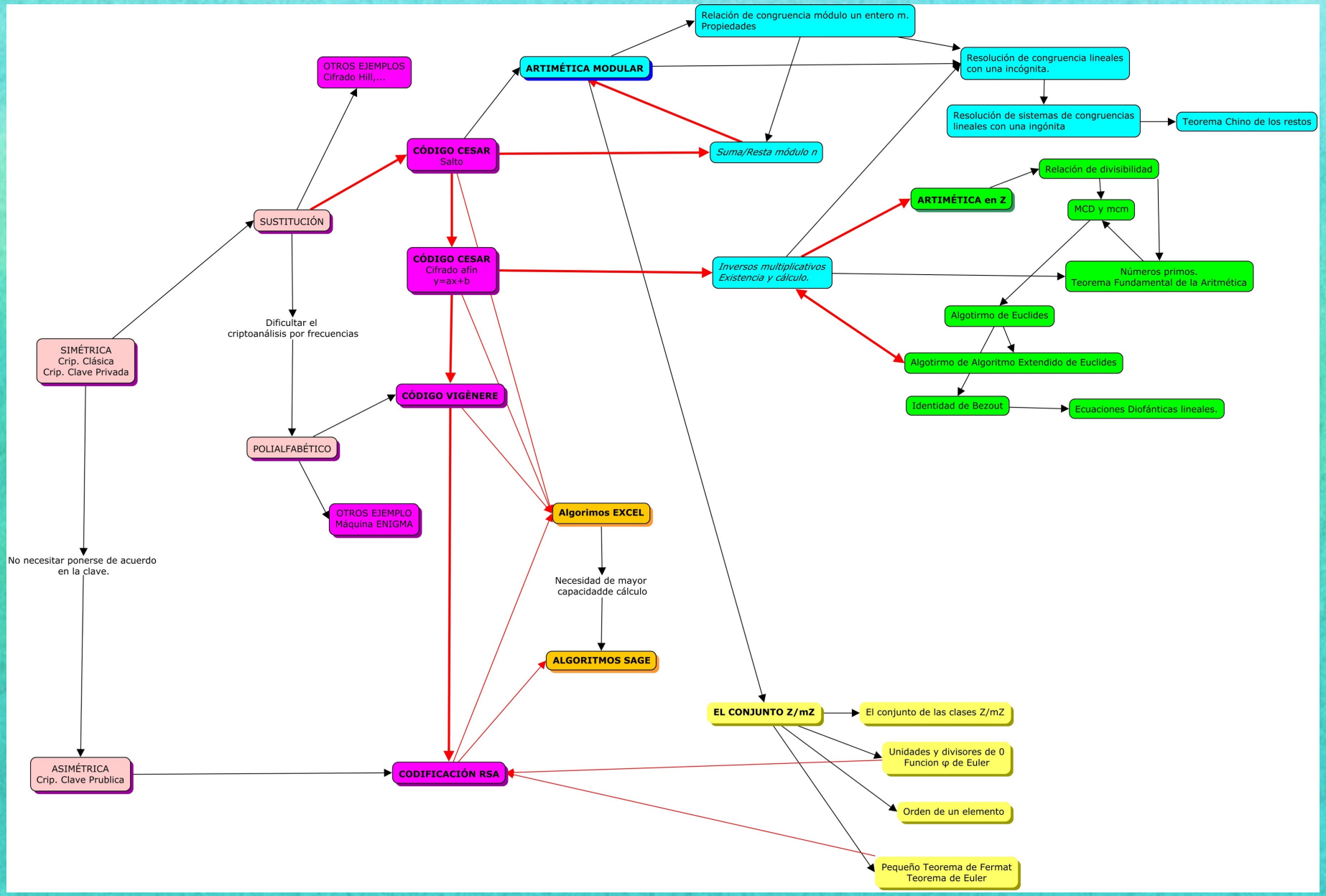
IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

4º ESO
MATEMÁTICAS PARA LA TOMA DE DECISIONES
Aritmética modular y criptografía.

Aunque los conocimientos abordados en esta materia tienen aplicaciones sobre elementos culturalmente muy recientes, lo cierto es que muchos de los objetos matemáticos considerados son relativamente antiguos. Por tanto, **el papel de la historia de las matemáticas puede ser relevante a distintos niveles** (Fauvel & Van Maanen, 2006). Para comenzar, puede resultar una fuente de motivación que contribuya además a trabajar aspectos socioemocionales y que permita poner en valor el carácter humano de las matemáticas. Además, también es posible utilizar la historia como fuente de problemas concretos y de situaciones introductorias de distintos conceptos. Finalmente, tampoco hay que descartar la posibilidad de que los estudiantes trabajen directamente sobre textos originales y fuentes históricas, si bien esto puede conllevar una labor de adaptación por parte del docente. En cualquier caso, para valorar la pertinencia o no de cualquiera de estos enfoques, deben tenerse en consideración los intereses particulares de los estudiantes, que pueden ser variables.

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO



Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

PLANIFICACIÓN SESIONES.

	SESIONES
1. Presentación del curso	1
2. Criptografía. Presentación. Sistemas de introducción.	1
3. Cifrados de Sustitución Simple. Cifrado Cesar	8
3.1. Presentación. Salto. Ejercicios sin uso de aritmética modular (Suma y resta). Programación en Excel.	1'5
3.2. Ejercicios con suma y resta módulo n. Programación en Excel.	1'5
3.3. Presentación salto afín. Concepto de inverso módulo	1
3.4. Calculo del inverso en aritmética modular. Existencia. MCD, Algoritmo de Euclides extendido.	2
3.5. Aritmética y Aritmética modular. Ecuaciones diofánticas. Sistemas de Congruencias,…	2
4. Cifrados de Sustitución Polialfabética. Código Vigenére	6
4.1. Presentación. Uso de la tabla. Ejercicios sencillos.	1'5
4.2. Algoritmo. Programación Excel.	1'5
4.3. Ejercicios	1
4.4. Otros sistemas polialfabéticos. Enigma	2
5. Cifrados Asimétricos. RSA.	8
5.1. Presentación.	1
5.2. Resultados teóricos: presentación. Función de Euler. Pequeño Teorema de Fermat. Teorema de Euler.	2
5.3. Algoritmo. Ejercicios sencillos	2
5.4. Programación. Excel. SAGE, Máxima,…	3

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

Criptografía

Kriptos: Oculto / Escondido

Graphos: Escribir

"ESCRITURA OCULTA"

(Ocultar el significado por un proceso de codificación)

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

Esteganografía

Steganos: Encubierto

Graphos: Escribir

“ESCRITURA OCULTA”

(Ocultar la existencia del mensaje)

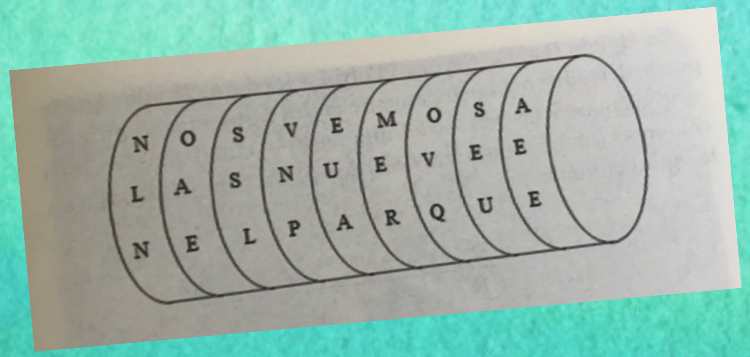
Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

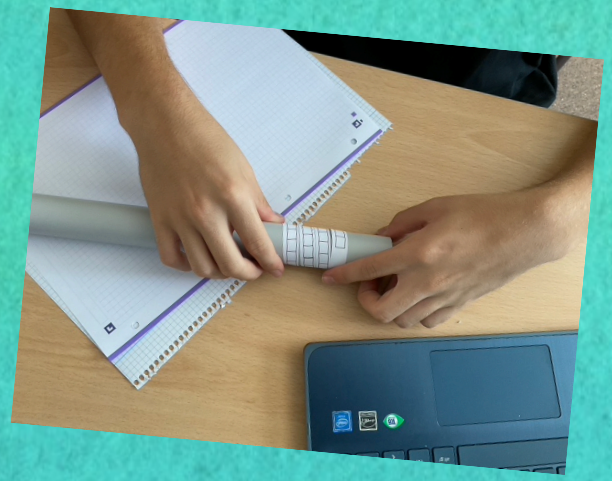
Facultad de Educación / Universidad de Zaragoza

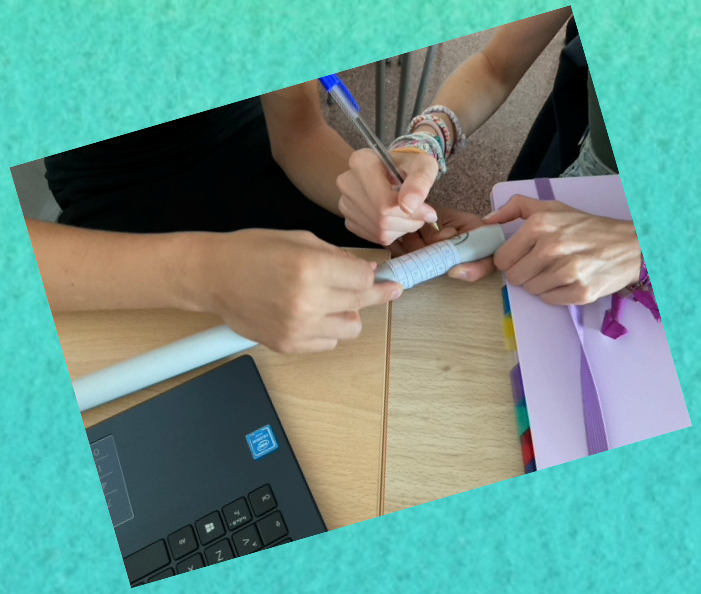
IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

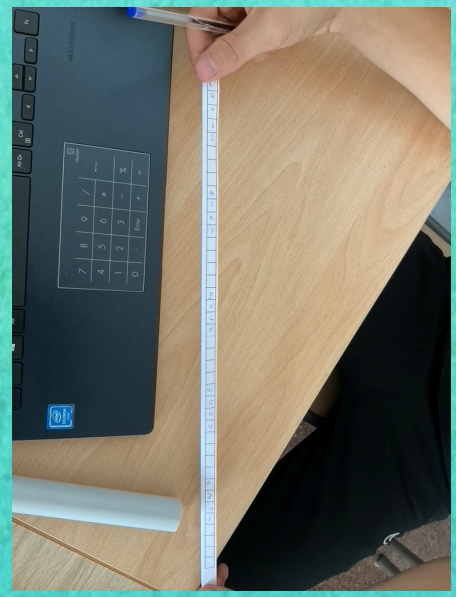
Esteganografía



Escítala espartana





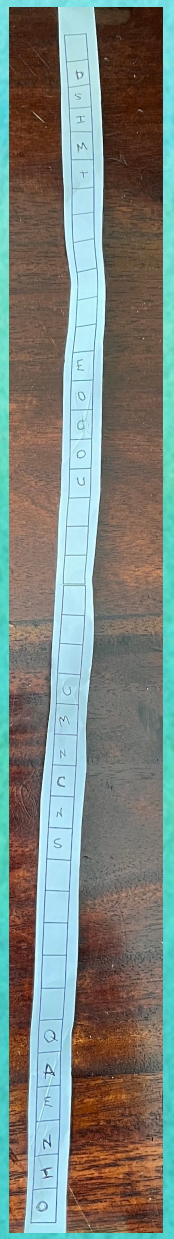


Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

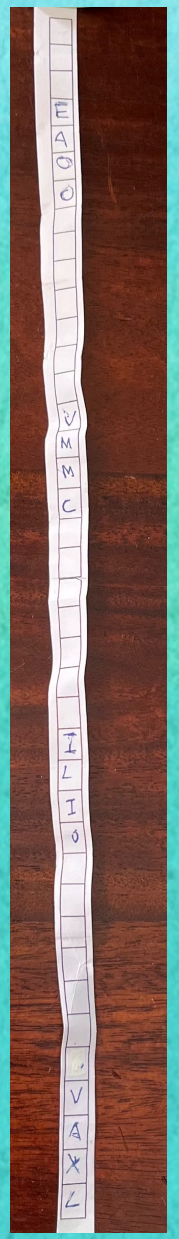
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO



Esteganografía

Escítala espartana



Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N (Ñ)	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

C	O	M	E	N	Z	A	M	O	S

13343215335511323443

SIGLO II a.n.e.

Historiador griego Polybios

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

Esteganografía / Criptografía

1.- CUESTIONARIO/RESUMEN ESTEGANOGRAFÍA.

Debes rellenar este cuestionario como resumen de la teoría y práctica que hemos realizado sobre esta parte del tema. Una vez relleno, guárdalo para utilizarlo a lo largo de la asignatura.

Todas las respuestas las hemos comentado en clase o están en el material de classroom.

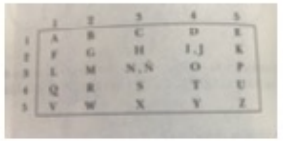
1.- ¿Qué es la esteganografía?

2.- ¿Qué es la criptografía?

3.- Señala cuatro métodos distintos de esteganografía. Explicalos brevemente

4.- ¿Se puede utilizar a la vez la esteganografía y la criptografía? Si es que sí, ¿puedes señalar una forma?

5.- Necesito mandar un mensaje. Si utilizo la siguiente tabla y cada letra la sustituyo por los números de sus coordenadas, por ejemplo, la M, por el 23, ¿estoy utilizando un método de criptografía o de esteganografía?



6.- Y si ahora mando el mismo mensaje pero utilizo esta otra tabla, de forma que donde hay un 1 pongo la primera letra del mensaje; donde hay un 2, pongo la segunda letra del mensaje;… ¿estoy utilizando un método de criptografía o de esteganografía?

2	18	13	10	27	11
25	8	7	23	30	5
35	14	1	34	19	36
9	31	22	28	3	29
21	26	16	6	24	17
15	4	32	20	12	33

7.- La escitala, ¿es un método de criptografía o de esteganografía? ¿En qué consiste?

8.- ¿Qué es lo fundamental para poder leer un mensaje que has recibido codificado con una escitala?

9.- ¿Hace falta otra escitala para leer un mensaje codificado con una o se puede leer de otra forma? ¿Qué necesitas saber?

Christian H. Martín Rubio. 4º ESO.

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

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
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	A	B

Recogido en la obra del historiador romano SUETONIO (c. 70- c. 126) que lleva por título *De vita Caesarum* (“*Vidas de los Césares)* (*ap. 121)*

Julio Cesar (100 a.c – 44 a.c.)

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE.

CÓDIGO CESAR

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
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	A	B

H	O	Y		E	S		M	A	R	T	E	S
J	Q	A		G	U		Ñ	C	T	V	G	U

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

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
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	A	B

N	B	C	J	U	X	B		N	V		L	Q	N	V	L	Q	J	B
E	S	T	A	M	O	S		E	N		C	I	E	N	C	I	A	S

N	B	C	J	U	X	B	N	V	L	Q	N	V	L	Q	J	B
E	S	T	A	M	O	S	E	N	C	I	E	N	C	I	A	S

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

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
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

N	B	C	J	U	X	B	N	V	L	Q	N	V	L	Q	J	B
E	S	T	A	M	O	S	E	N	C	I	E	N	C	I	A	S

9																										
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

Salto: 7

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

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	F	G
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6

P	U	E	D	E	S	L	E	E	R	E	S	T	E	M	E	N	S	A	J	E
W	B	L	K	L	Z	R	L	L	Y	L	Z	A	L	S	L	T	Z	H	P	L

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

Salto: 9

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8

L	T	J	A	X	Z	D	N	T	N	X	U	N	V	B	J	R	N	B	X	L	D	T	C	X	B
C	L	A	R	O	Q	U	E	L	E	O	M	E	N	S	A	J	E	S	O	C	U	L	T	O	S

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

Salto: 10

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	0	1	2	3	4	5	6	7	8	9

V	A	M	O	S	A	A	C	A	B	A	R	C	O	N	C	E	S	A	R	B	A	S	I	C	O
F	K	V	Y	C	K	K	M	K	L	K	B	M	Y	W	M	Ñ	C	K	B	L	K	C	R	M	Y

Z	Ñ	B	Y	Q	K	I	Y	D	B	Y	M	Ñ	C	K	B	M	Y	W	M	R	O	B	K	N	Y	K	O	R	W
P	E	R	O	H	A	Y	O	T	R	O	C	E	S	A	R	C	O	N	C	I	F	R	A	D	O	A	F	I	N

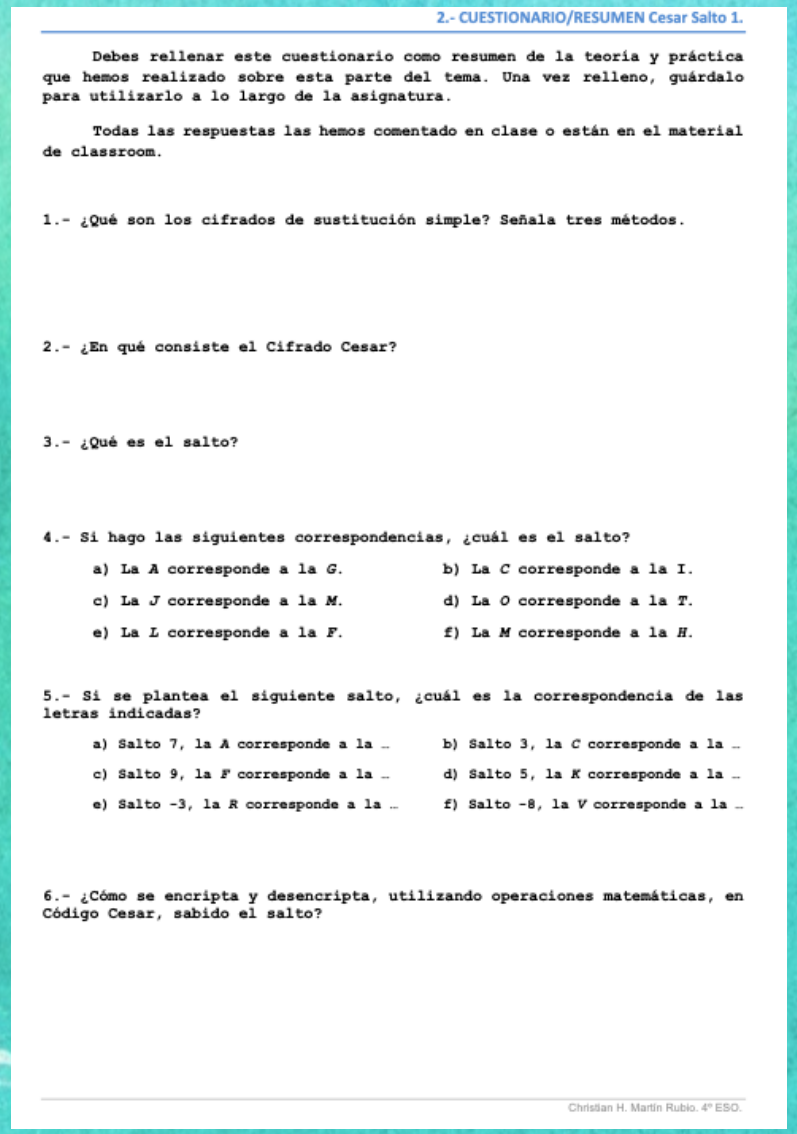
Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE. CÓDIGO CESAR



2.- CUESTIONARIO/RESUMEN Cesar Salto 1.

Debes rellenar este cuestionario como resumen de la teoría y práctica que hemos realizado sobre esta parte del tema. Una vez relleno, guárdalo para utilizarlo a lo largo de la asignatura.

Todas las respuestas las hemos comentado en clase o están en el material de classroom.

1.- ¿Qué son los cifrados de sustitución simple? Señala tres métodos.

2.- ¿En qué consiste el Cifrado Cesar?

3.- ¿Qué es el salto?

4.- Si hago las siguientes correspondencias, ¿cuál es el salto?

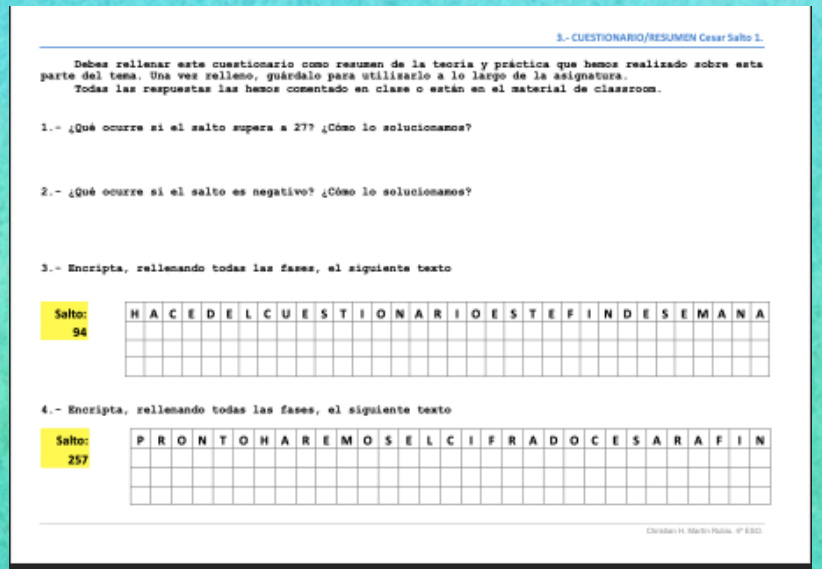
a) La *A* corresponde a la *G*.
b) La *C* corresponde a la *I*.
c) La *J* corresponde a la *M*.
d) La *O* corresponde a la *T*.
e) La *L* corresponde a la *F*.
f) La *M* corresponde a la *H*.

5.- Si se plantea el siguiente salto, ¿cuál es la correspondencia de las letras indicadas?

a) Salto 7, la *A* corresponde a la …
b) Salto 3, la *C* corresponde a la …
c) Salto 9, la *F* corresponde a la …
d) Salto 5, la *K* corresponde a la …
e) Salto -3, la *R* corresponde a la …
f) Salto -8, la *V* corresponde a la …

6.- ¿Cómo se encripta y desencripta, utilizando operaciones matemáticas, en Código Cesar, sabido el salto?

Christian H. Martín Rubio. 4º ESO.



3.- CUESTIONARIO/RESUMEN Cesar Salto 1.

Debes rellenar este cuestionario como resumen de la teoría y práctica que hemos realizado sobre esta parte del tema. Una vez relleno, guárdalo para utilizarlo a lo largo de la asignatura.
Todas las respuestas las hemos comentado en clase o están en el material de classroom.

1.- ¿Qué ocurre si el salto supera a 27? ¿Cómo lo solucionamos?

2.- ¿Qué ocurre si el salto es negativo? ¿Cómo lo solucionamos?

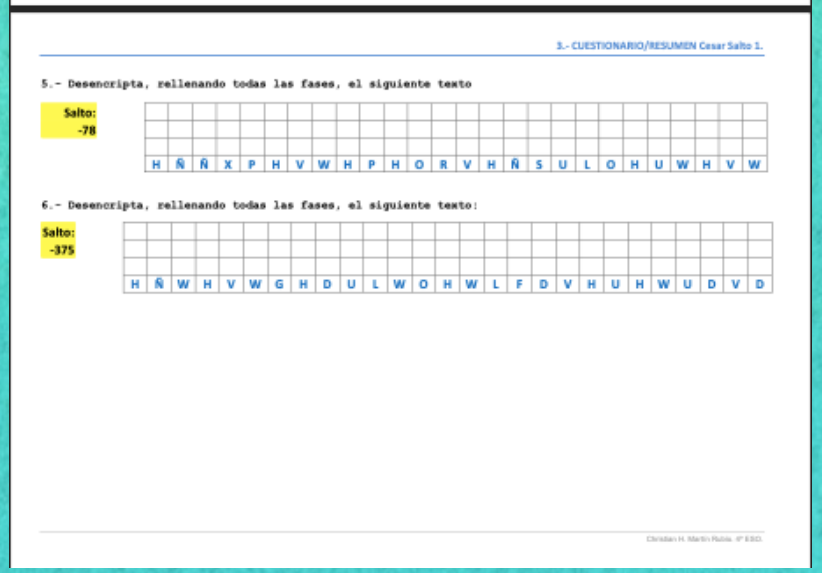
3.- Encripta, rellenando todas las fases, el siguiente texto

Salto: 94	H	A	C	E	D	E	L	C	U	E	S	T	I	O	N	A	R	I	O	E	S	T	E	F	I	N	D	E	S	E	M	A	N	A

4.- Encripta, rellenando todas las fases, el siguiente texto

Salto: 257	P	R	O	N	T	O	H	A	R	E	M	O	S	E	L	C	I	F	R	A	D	O	C	E	S	A	R	A	F	I	N

Christian H. Martín Rubio. 4º ESO.



3.- CUESTIONARIO/RESUMEN Cesar Salto 1.

5.- Desencripta, rellenando todas las fases, el siguiente texto

Salto: -78																															
	H	Ñ	Ñ	X	P	H	V	W	H	P	H	O	R	V	H	Ñ	S	U	L	O	H	U	W	H	V	W					

6.- Desencripta, rellenando todas las fases, el siguiente texto:

Salto: -375																															
	H	Ñ	W	H	V	W	G	H	D	U	L	W	O	H	W	L	F	D	V	H	U	H	W	U	D	V	D				

4.- CUESTIONARIO/RESUMEN Aritmética Modular.

Debes rellenar este cuestionario como resumen de la teoría y práctica que hemos realizado sobre esta parte del tema. Una vez relleno, guárdalo para utilizarlo a lo largo de la asignatura.
Todas las respuestas las hemos comentado en clase o están en el material de classroom.

1.- ¿Qué significa que [illegible]?

2.- Demuestra que si [illegible] y [illegible], entonces se cumple que [illegible].

3.- Demuestra que si [illegible] entonces se cumple que [illegible].

4.- Demuestra que si [illegible] entonces se cumple que [illegible] para [illegible].

5.- Construye la tabla de sumar módulo 7.

6.- Construye la tabla de restar módulo 7.

7.- Resuelve las siguientes congruencias:

[illegible]

8.- Si [illegible] y [illegible], resuelve las siguientes congruencias:

[illegible]

9.- Si [illegible], calcula x para que sean ciertas las siguientes congruencias:

[illegible]

4.- CUESTIONARIO/RESUMEN Aritmética Modular.

10.- Si ahora son las 15:00h, ¿qué hora será dentro de 218 horas?

11.- Si hoy es lunes, ¿qué día de la semana será dentro de 159 días?

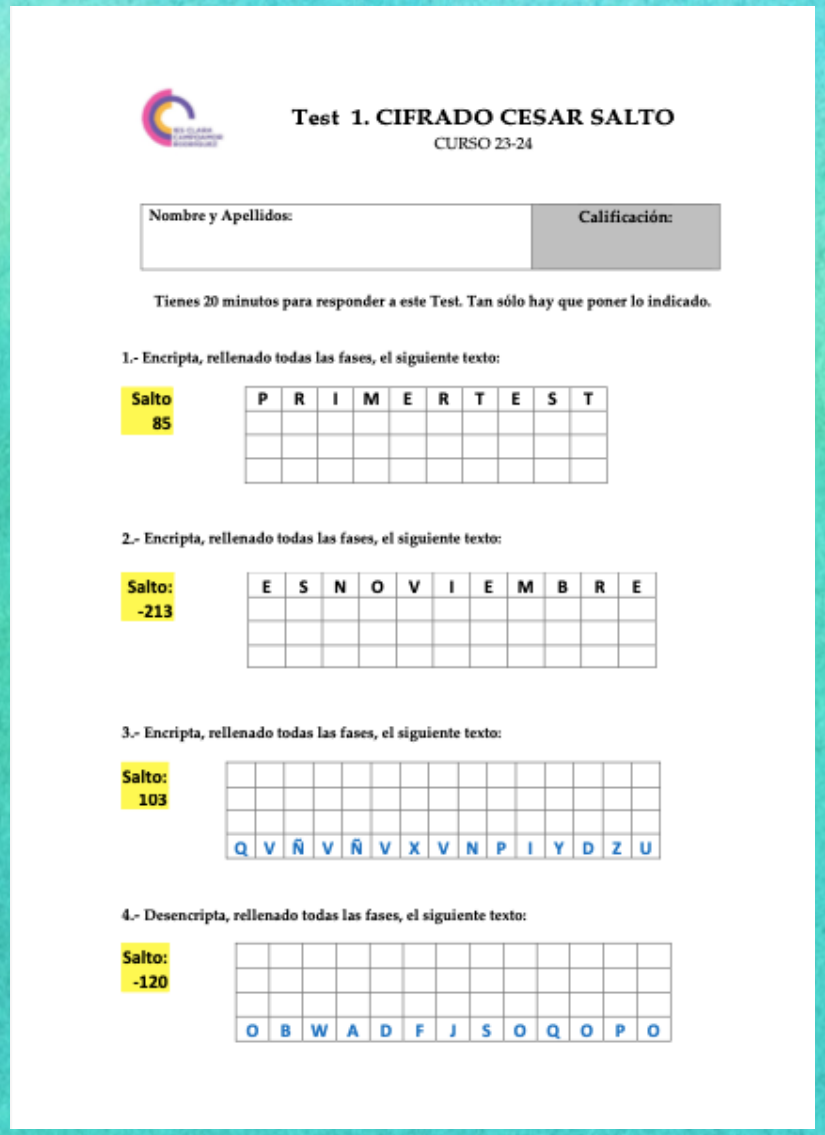
12.- Si esta mes es noviembre, ¿qué mes será dentro de 317 meses?

13.- Demuestra, para un número de 4 cifras, el criterio de divisibilidad del 2, del 3, del 4 y del 5.

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE. CÓDIGO CESAR



Test 1. CIFRADO CESAR SALTO
CURSO 23-24

Nombre y Apellidos:	Calificación:

Tienes 20 minutos para responder a este Test. Tan sólo hay que poner lo indicado.

1.- Encripta, rellenado todas las fases, el siguiente texto:

Salto 85

P	R	I	M	E	R	T	E	S	T

2.- Encripta, rellenado todas las fases, el siguiente texto:

Salto: -213

E	S	N	O	V	I	E	M	B	R	E

3.- Encripta, rellenado todas las fases, el siguiente texto:

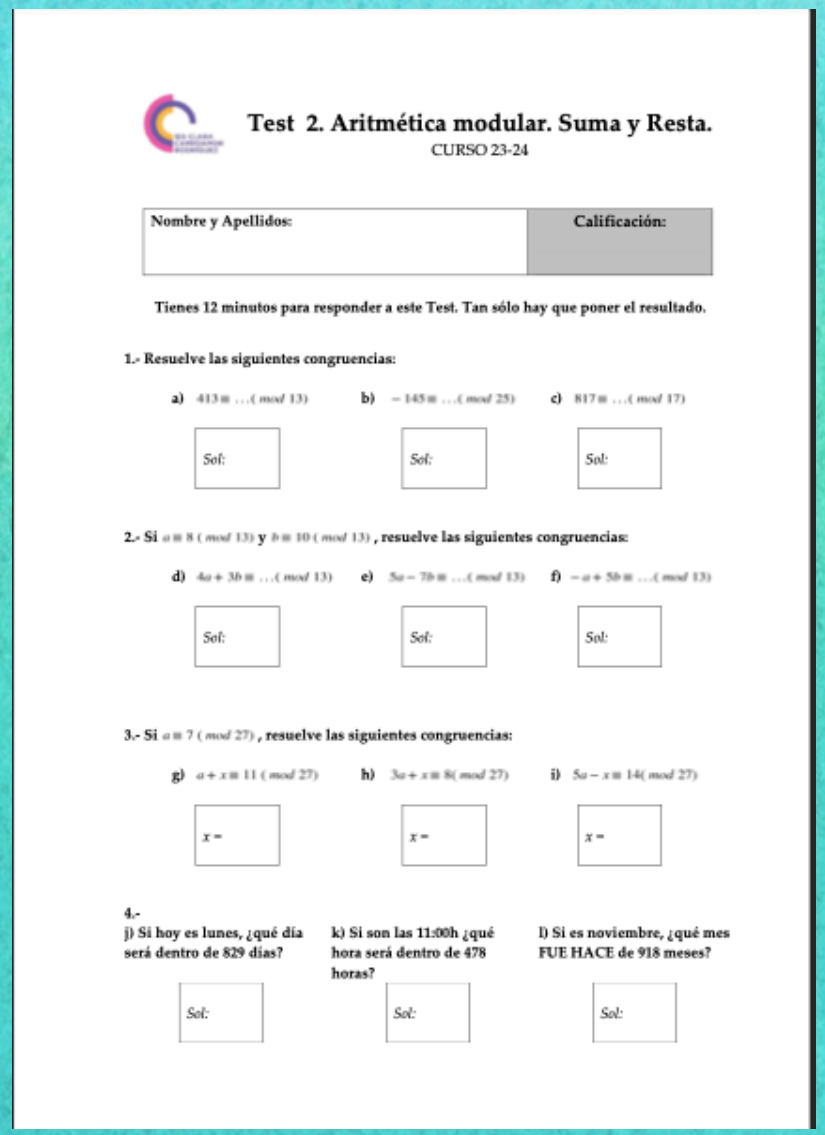
Salto: 103

Q	V	Ñ	V	Ñ	V	X	V	N	P	I	Y	D	Z	U

4.- Desencripta, rellenado todas las fases, el siguiente texto:

Salto: -120

O	B	W	A	D	F	J	S	O	Q	O	P	O	



Test 2. Aritmética modular. Suma y Resta.
CURSO 23-24

Nombre y Apellidos:	Calificación:

Tienes 12 minutos para responder a este Test. Tan sólo hay que poner el resultado.

1.- Resuelve las siguientes congruencias:

a) $413 \equiv \ldots (mod\ 13)$ b) $-145 \equiv \ldots (mod\ 25)$ c) $817 \equiv \ldots (mod\ 17)$

Sol: Sol: Sol:

2.- Si $a \equiv 8\ (mod\ 13)$ y $b \equiv 10\ (mod\ 13)$, resuelve las siguientes congruencias:

d) $4a + 3b \equiv \ldots (mod\ 13)$ e) $5a - 7b \equiv \ldots (mod\ 13)$ f) $-a + 5b \equiv \ldots (mod\ 13)$

Sol: Sol: Sol:

3.- Si $a \equiv 7\ (mod\ 27)$, resuelve las siguientes congruencias:

g) $a + x \equiv 11\ (mod\ 27)$ h) $3a + x \equiv 8 (mod\ 27)$ i) $5a - x \equiv 14 (mod\ 27)$

$x =$ $x =$ $x =$

4.-
j) Si hoy es lunes, ¿qué día será dentro de 829 días?
k) Si son las 11:00h ¿qué hora será dentro de 478 horas?
l) Si es noviembre, ¿qué mes FUE HACE de 918 meses?

Sol: Sol: Sol:

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

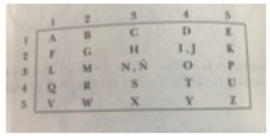
CIFRADOS DE SUSTITUCIÓN SIMPLE. CÓDIGO CESAR

Examen 1. Cifrados básicos y Suma y Resta modular
CURSO 23-24

Nombre y Apellidos:	Calificación:

Hay que razonar y justificar todos los pasos e incluir todas las operaciones. Hay que poner el nombre y apellidos. Si no, no se podrá valorar el examen.

1.- (1 punto) Necesito mandar un mensaje. Si utilizo la siguiente tabla y cada letra la sustituyo por los números de sus coordenadas, por ejemplo, la M, por el 23, ¿estoy utilizando un método de criptografía o de esteganografía?



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N, Ñ	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Codifica con este método la frase:

COMENZAMOS

2.- (0'5 puntos) ¿Hace falta otra escítala para leer un mensaje codificado con una o se puede leer de otra forma? ¿Qué necesitas saber?

3.- (0'5 puntos) ¿Cómo se encripta y desencripta, utilizando operaciones matemáticas, en Código Cesar, sabido el salto?

4.- (1 punto)

a) Si hago las siguientes correspondencias, ¿cuál es el salto?

a.1) La *J* corresponde a la *R*.

a.2) La *M* corresponde a la *F*.

b) Si se plantea el siguiente salto, ¿cuál es la correspondencia de las letras indicadas?

b.1) Salto *8*, la *V* corresponde a la ...

b.2) Salto *-8*, la *V* corresponde a la ...

5.- (1'5 puntos) Encripta, rellenando todas las fases, los siguientes textos:

Salto: 19 C O M I E N Z A S O T R A P A R T E

Salto: -89 V A S A S A C A R U N D I E Z

6.- (2'5 puntos) Desencripta, rellenando todas las fases, los siguientes textos:

Salto: 14

M Ñ S Ñ Y H Ñ D C P C

Salto: -95

N T B E N N E U G Y Q G U O N

7.- (0'5 puntos) Demuestra que si $a \equiv b \pmod n$ y $c \equiv d \pmod n$, entonces se cumple que $a + c \equiv b + d \pmod n$.

8.- (2 puntos)

a) Resuelve las siguientes congruencias:

a.1) $-217 \equiv \ldots \pmod{17}$ a.2) $1256 \equiv \ldots \pmod{21}$

b) Si $a \equiv 8 \pmod{27}$ y $b \equiv 22 \pmod{27}$, resuelve las siguientes congruencias:

b.1) $-7a - 2b \equiv \ldots \pmod{27}$ b.2) $3a + 2b \equiv \ldots \pmod{27}$

c) Si $a \equiv 7 \pmod{27}$, resuelve las siguientes congruencias:

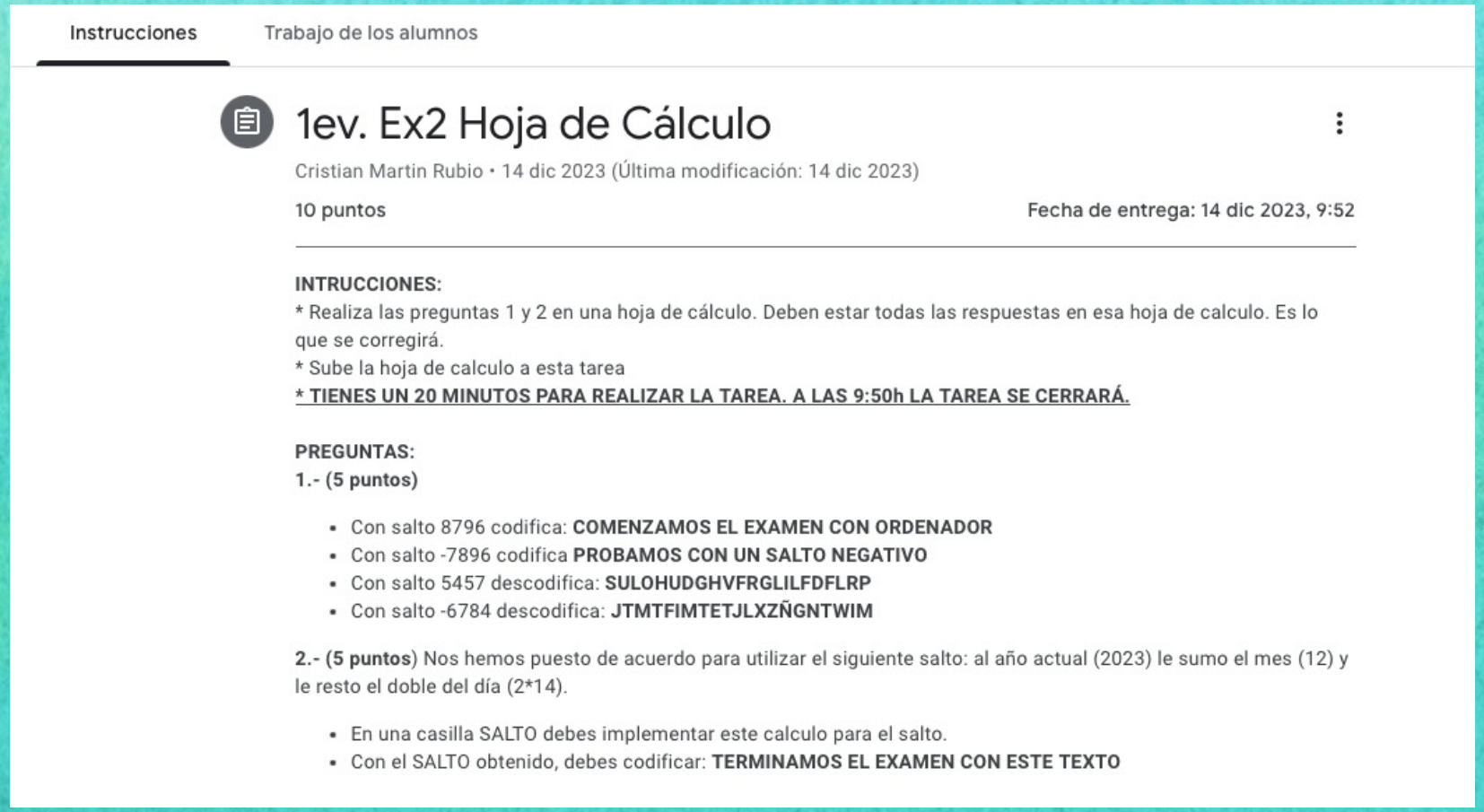
c.1) $-3a - x \equiv 8 \pmod{27}$ c.2 $9a + x \equiv 7 \pmod{27}$

9.- (0'5 puntos) Si estamos en otoño, ¿qué estación será dentro de 519 estaciones?

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE. CÓDIGO CESAR



Instrucciones | Trabajo de los alumnos

1ev. Ex2 Hoja de Cálculo

Cristian Martin Rubio • 14 dic 2023 (Última modificación: 14 dic 2023)

10 puntos — Fecha de entrega: 14 dic 2023, 9:52

INTRUCCIONES:
* Realiza las preguntas 1 y 2 en una hoja de cálculo. Deben estar todas las respuestas en esa hoja de calculo. Es lo que se corregirá.
* Sube la hoja de calculo a esta tarea
*** TIENES UN 20 MINUTOS PARA REALIZAR LA TAREA. A LAS 9:50h LA TAREA SE CERRARÁ.**

PREGUNTAS:
1.- (5 puntos)

- Con salto 8796 codifica: **COMENZAMOS EL EXAMEN CON ORDENADOR**
- Con salto -7896 codifica **PROBAMOS CON UN SALTO NEGATIVO**
- Con salto 5457 descodifica: **SULOHUDGHVFRGLILFDFLRP**
- Con salto -6784 descodifica: **JTMTFIMTETJLXZÑGNTWIM**

2.- (5 puntos) Nos hemos puesto de acuerdo para utilizar el siguiente salto: al año actual (2023) le sumo el mes (12) y le resto el doble del día (2*14).

- En una casilla SALTO debes implementar este calculo para el salto.
- Con el SALTO obtenido, debes codificar: **TERMINAMOS EL EXAMEN CON ESTE TEXTO**

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

a=7; b=1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Y	A	M	E	S	T	A	G	U	S	T	A	N	D	O	E	S	T	O
Ñ	B	E	C	Z	G	B	P	N	Z	G	B	L	V	Y	C	Z	G	Y

P	C	L	D	B	X	F	B	S	B	N	L	Z	B	I	B	V	Y
G	E	N	I	A	L	P	A	R	A	U	N	S	A	B	A	D	O

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

a=3; b=1

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

H	K	Y	K	B	K	S	N	S	P	K	N	H	Y	S	N	B	E	Y	N	K	V	B	N

G	J	X	J	A	J	R	M	R	O	J	M	G	X	R	M	A	D	X	M	J	U	A	M

C	U	I	D	A	D	O	N	O	F	U	N	C	I	O	N	A	S	I	E	M	P	R	E
H	K	Y	K	B	K	S	N	S	P	K	N	H	Y	S	N	B	E	Y	N	K	V	B	N

CUIDADO: 3 no es primo con 27

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

a=11; b=8

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

A	H	O	R	A	S	I	Q	U	E	P	A	S	A	M	O	S	A	O	T	R	O	M	E	T	O	D	O
I	E	L	Q	I	B	O	G	W	Y	V	I	B	I	F	L	B	I	L	M	Q	L	F	Y	M	L	Ñ	L

V	W	Y	B	N	I	M	Y	P	T	L	T	I	P	I	B	Ñ	Y	I	U	F	L	Q	X	I	Q
P	U	E	S	Y	A	T	E	N	G	O	G	A	N	A	S	D	E	A	L	M	O	R	Z	A	R

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CRIPTOGRAFIA CON MATRICES

MÉTODO HILL

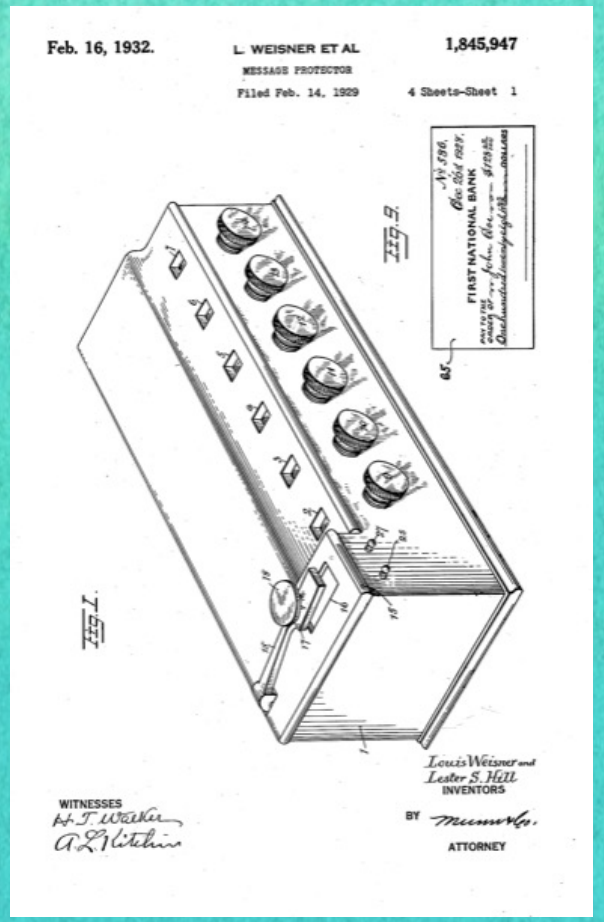
Lester S. Hill (1891-1961)

Cryptography in an Algebraic Alphabet (1929)

American Mathematical Monthly

$$A \cdot X = Y$$

$$X = A^{-1} \cdot Y$$


Feb. 16, 1932. L. WEISNER ET AL 1,845,947
MESSAGE PROTECTOR
Filed Feb. 14, 1929 4 Sheets-Sheet 1
FIRST NATIONAL BANK
Louis Weisner and Lester S. Hill INVENTORS
WITNESSES
ATTORNEY

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

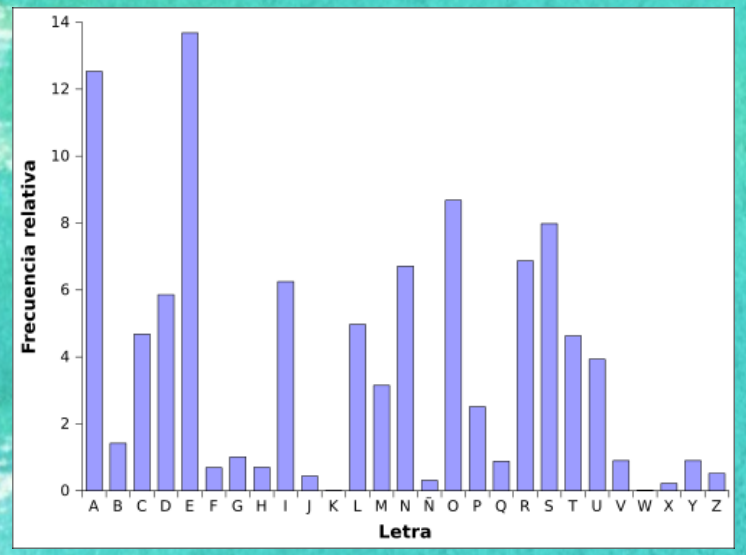
IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

W	F		W	L	M	S		U	D	S	L	W		W	E	I	W	R	S	K	W		U	H	F		U	W	L	S	K



Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Porcentaje	12,53%	1,42%	4,68%	5,86%	13,68%	0,69%	1,01%	0,70%	6,25%	0,44%	0,02%	4,97%	3,15%	6,71%
Letra	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Porcentaje	0,31%	8,68%	2,51%	0,88%	6,87%	7,98%	4,63%	3,93%	0,90%	0,01%	0,22%	0,90%	0,52%	

E, A, O, S, R, N, I, D, L, C, T, U, M, P, B, G, V, Y, Q, H, F, Z, J, Ñ, X, K, W.

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN SIMPLE

CÓDIGO CESAR

Salto: 19

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

W	F		W	L	M	S		U	D	S	L	W		W	E	I	W	R	S	K	W		U	H	F		U	W	L	S	K
E			E									E		E			E				E							E			
E	N		E	S	T	A		C	L	A	S	E		E	M	P	E	Z	A	R	E		C	O	N		C	E	S	A	R

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Porcentaje	12,53%	1,42%	4,68%	5,86%	13,68%	0,69%	1,01%	0,70%	6,25%	0,44%	0,02%	4,97%	3,15%	6,71%
Letra	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Porcentaje	0,31%	8,68%	2,51%	0,88%	6,87%	7,98%	4,63%	3,93%	0,90%	0,01%	0,22%	0,90%	0,52%	

E, A, O, S, R, N, I, D, L, C, T, U, M, P, B, G, V, Y, Q, H, F, Z, J, Ñ, X, K, W.

W	7		U	3		K	2
F	2		D	1		H	1
L	3		E	1			
M	1		I	1			
S	4		R	1			

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

Blaise de Vigenère

(1523-1596)

Traicté des Chiffres ou secrètes manières d'écrire (1586)

Giovan Battista Belalso

(1553)

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		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
0	A	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
1	B	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	a
2	C	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	a	b
3	D	d	e	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
4	E	e	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
5	F	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
6	G	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	f
7	H	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	f	g
8	I	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	J	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	K	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	L	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	M	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	N	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	Ñ	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ
16	P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o
17	Q	q	r	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
18	R	r	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
19	S	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
20	T	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	s
21	U	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	s	t
22	V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u
23	W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v
24	X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w
25	Y	y	z	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
26	Z	z	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

COLUMNAS: Letras del mensaje

FILAS: Letras de las palabra clave

O	T	R	O		C	I	F	R	A	D	O
O	L	S	O		S	O	L	S	O	L	S

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
		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
0	A	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
1	B	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	a
2	C	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	a	b
3	D	d	e	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
4	E	e	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
5	F	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
6	G	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	f
7	H	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	f	g
8	I	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	J	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	K	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
11	L	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
12	M	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
13	N	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
14	Ñ	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
15	O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ
16	P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o
17	Q	q	r	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
18	R	r	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
19	S	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
20	T	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	s
21	U	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	s	t
22	V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u
23	W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v
24	X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w
25	Y	y	z	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
26	Z	z	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

COLUMNAS: Letras del mensaje
FILAS: Letras de las palabra clave

O	T	R	O		C	I	F	R	A	D	O
O	L	S	O		S	O	L	S	O	L	S

D	E	K	D		U	W	P	K	O	Ñ	H

Clave: SOL

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

O	T	R	O	M	E	T	O	D	O	D	E	C	R	I	P	T	O	G	R	A	F	I	A
L	S	O	L	S	O	L	S	O	L	S	O	L	S	O	L	S	O	L	S	O	L	S	O
Z	M	G	Z	E	S	E	H	R	Z	V	S	N	K	W	A	M	D	Q	K	O	P	A	O

Clave: SOL

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

L	S	I	J	O	V	S	L	U	D	C	M	O	C	W	Z	A	K	D	N	W	H	Z
S	O	S	O	L	S	O	L	S	O	L	S	O	L	S	O	L	S	O	L	S	O	L
S	E	P	U	E	D	E	A	C	O	R	T	A	R	E	L	P	R	O	C	E	S	O

Clave: SOL

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

4	19	4	11	19	4	6	21	13	3	15
E	S	E	L	S	E	G	U	N	D	O
S	O	S	O	L	S	O	L	S	O	L
19	15	19	15	11	19	15	11	19	15	11
23	34	23	26	30	23	21	32	32	18	26
23	7	23	26	3	23	21	5	5	18	26
W	H	W	Z	D	W	U	F	F	R	Z

19	15	19	15	11	19	15	11	19	15	11
S	O	S	O	L	S	O	L	S	O	L
W	H	W	Z	D	W	U	F	F	R	Z
23	7	23	26	3	23	21	5	5	18	26
4	-8	4	11	-8	4	6	-6	-14	3	15
4	19	4	11	19	4	6	21	13	3	15
E	S	E	L	S	E	G	U	N	D	O

Clave: SOL

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

19	15	12	15	19	21	13	4	24	2	4	11	4	13	20	4	6	18	21	16	15	3	4	2	18	8	16	20	15	6	18	0	5	0	19
S	O	M	O	S	U	N	E	X	C	E	L	E	N	T	E	G	R	U	P	O	D	E	C	R	I	P	T	O	G	R	A	F	A	S

T	E	I	C	S	M	A	T	E	I	C	S	M	A	T	E	I	C	S	M	A	T	E	I	C	S	M	A	T	E	I	C	S	M	A
20	4	8	2	19	12	0	20	4	8	2	19	12	0	20	4	8	2	19	12	0	20	4	8	2	19	12	0	20	4	8	2	19	12	0
39	19	20	17	38	33	13	24	28	10	6	30	16	13	40	8	14	20	40	28	15	23	8	10	20	27	28	20	35	10	26	2	24	12	19
12	19	20	17	11	6	13	24	1	10	6	3	16	13	13	8	14	20	13	1	15	23	8	10	20	0	1	20	8	10	26	2	24	12	19
M	S	T	Q	L	G	N	X	B	K	G	D	P	N	N	I	Ñ	T	N	B	O	W	I	K	T	A	B	T	I	K	Z	C	X	M	S

Clave: MATEMATICAS, 2

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

CIFRADO VIGENÈRE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

4	12	0	20	4	8	2	19	12	0	20	4	8	2	19	12	0	20	4	8	2	19	12	0	20	4	8	2	19	12	0	20
E	M	A	T	E	I	C	S	M	A	T	E	I	C	S	M	A	T	E	I	C	S	M	A	T	E	I	C	S	M	A	T
C	Ñ	O	F	S	Y	W	W	O	A	F	S	A	R	S	D	A	K	Y	M	Ñ	W	O	E	M	O	I	E	D	M	V	X
2	14	15	5	19	25	23	23	15	0	5	19	0	18	19	3	0	10	25	12	14	23	15	4	12	15	8	4	3	12	22	24
-2	2	15	-15	15	17	21	4	3	0	-15	15	-8	16	0	-9	0	-10	21	4	12	4	3	4	-8	11	0	2	-16	0	22	4
25	2	15	12	15	17	21	4	3	0	12	15	19	16	0	18	0	17	21	4	12	4	3	4	19	11	0	2	11	0	22	4
Y	C	O	M	O	Q	U	E	D	A	M	O	S	P	A	R	A	Q	U	E	M	E	D	E	S	L	A	C	L	A	V	E

Clave: MATEMATICAS, 2

Christian H. Martín Rubio

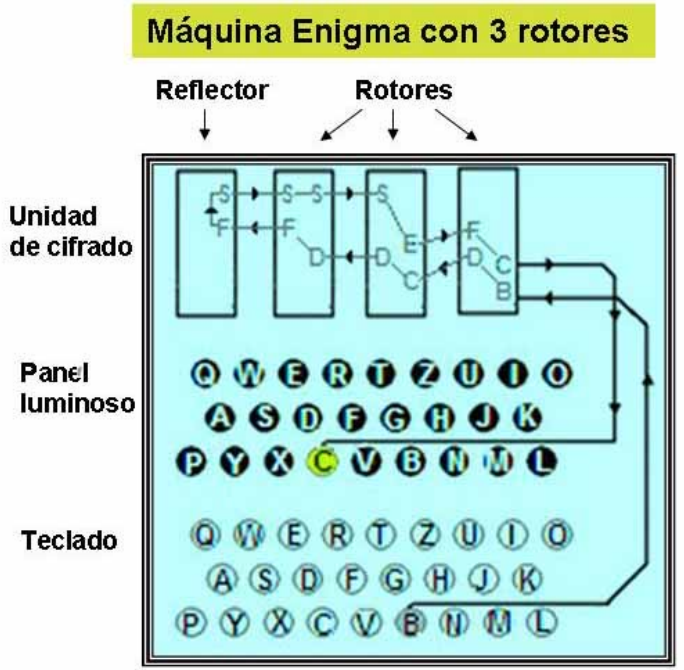
IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS DE SUSTITUCIÓN POLIALFABÉTICA

MAQUINA ENIGMA



Christian H. Martín Rubio

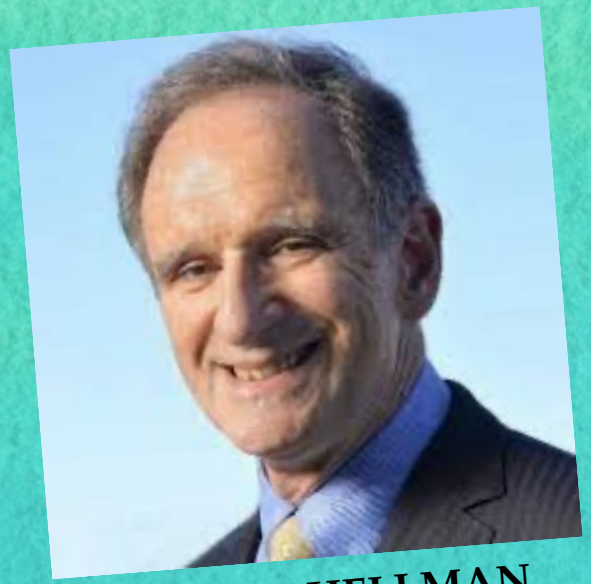
IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS ASIMÉTRICOS. CLAVE PÚBLICA.

WHITFIELD DIFFIE
(1944 -)



MARTIN HELLMAN
(1945 -)

"News Directions in Cryptography"
(1976)

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—**Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is a multiple access cipher. A private conversation can therefore be held between any two individuals regardless of

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

1. FUNCIÓN EULER: Dado n un número entero positivo, se define, $\phi(n)$ como la cantidad de enteros positivos menores que n y coprimos con él.

2. Si $n = p \cdot q$,con p y q dos primos distintos, entonces $\phi(n) = (p-1) \cdot (q-1)$.

3. PEQUEÑO TEOREMA DE FERMAT: Si $(a, p) = 1$, p primo, entonces $a^p \equiv a \pmod{p}$. O lo que es lo mismo: $a^{p-1} \equiv 1 \pmod{p}$

4. TEOREMA DE EULER: Si $(n, a) = 1$, entonces $a^{\phi}(n) \equiv 1 \pmod{n}$

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

IFRN ZYNM QWXM ONIB IKNM AOHK WSZZ JT … en 4° ESO

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

CIFRADO RSA:

Se toman p y q dos números primos -estos números son los números RSA-.

Hacemos $n = p \cdot q$. Sabemos que $\phi(n) = (p-1) \cdot (q-1)$

Tomamos un número e tal que $(\phi(n), e) = 1$.

CLAVE PÚBLICA: (n, e)

CLAVE PRIVADA: d tal que $d \equiv e^{-1} \pmod{\phi(n)}$

Cualquier persona utiliza la clave pública (n, e),para encriptar un mensaje m, haciendo $M \equiv m^e \pmod{n}$.

Se lo envía a la persona en particular, que lo desencripta haciendo: $M^d \pmod{n}$.

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

Tomamos **p=3** y **q=11**.

n=3·11; **n=33** Φ (n)=2·10; **Φ (n)=20** Tomo un primo con 20, **e=7**

CLAVE PÚBICA: (33,7) **CLAVE PRIVADA: d=3** [$d \equiv 7^{-1} (\mathrm{mod}(20))$]

MARTA me quiere mandar un mensaje que es **9** (m=9).

Hace: $M \equiv 9^7 (\mathrm{mod}\ 33)$ $M \equiv 4782969\ (\mathrm{mod}\ 33)$ $M \equiv 15\ (\mathrm{mod}\ 33)$….**Me envía el 15**

YO, al recibir el 15, hago: $15^3\ (\mathrm{mod}\ 33) \equiv 3375\ (\mathrm{mod}\ 33) \equiv 9\ (\mathrm{mod}\ 33)$….**Obtengo el mensaje 9 original**

EL MENSAJE *m* A ENVIAR DEBE SER MENOR QUE *n*

Christian H. Martín Rubio
IES Clara Campoamor Rodríguez, Zaragoza
Facultad de Educación / Universidad de Zaragoza

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

p=3 y q=11; (33,3)

S	A	B	A	D	O
19	0	1	0	3	15
6859	0	1	0	27	3375
28	**0**	**1**	**0**	**27**	**9**

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

p=3 y q=11; (33,3)

22	3	31	12	0
2E+09	2187	3E+10	4E+07	0
22	9	4	12	0
V	J	E	M	A

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

p=5 y q=3; (15,5)

H	O	L	A
7	0	11	0
H	A	L	A

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

CIFRADOS ASIMÉTRICOS. CIRADO RSA.

p=7 y q=5; (35,5)

0	32	0	1	0	17	15	24
0	3E+07	0	1	0	1419857	8E+05	8E+06
0	2	0	1	0	12	15	19
A	C	A	B	A	M	O	S

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza

¡¡¡MUCHAS GRACIAS!!!

Christian H. Martín Rubio

IES Clara Campoamor Rodríguez, Zaragoza

Facultad de Educación / Universidad de Zaragoza