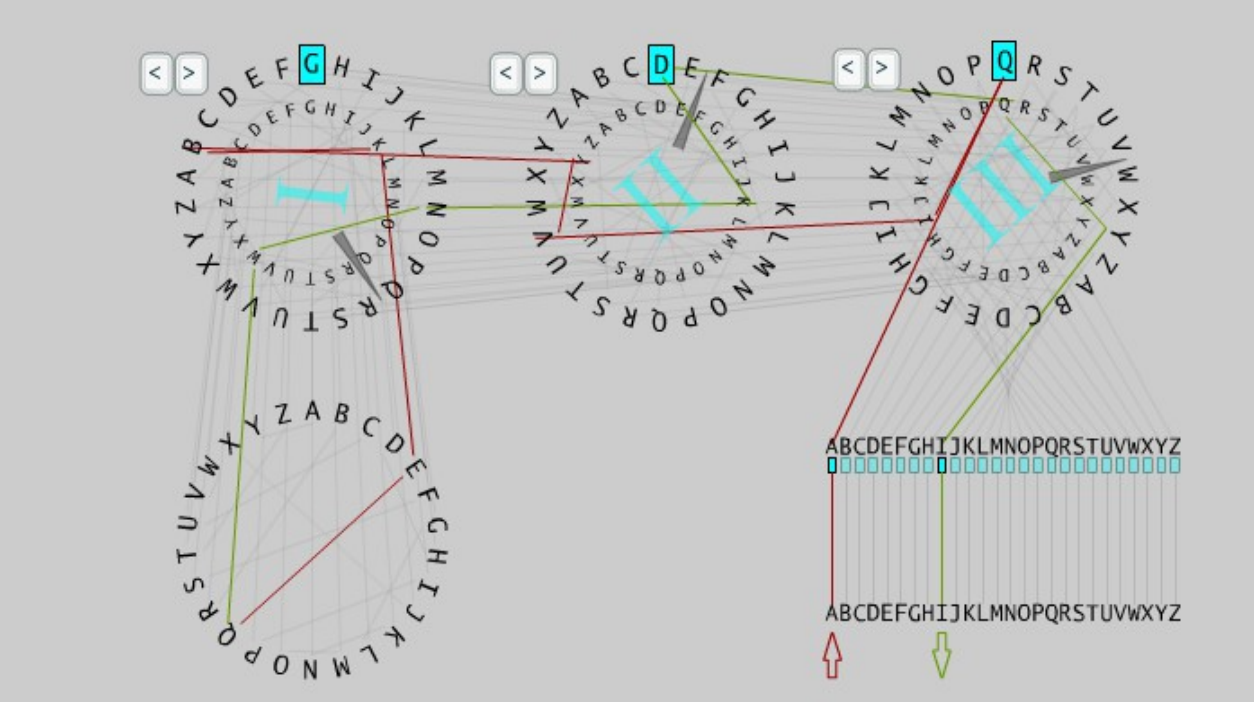
PROJECTE FINAL DE CARRERA 2013/14 – 2

ENGINYERIA TÈCNICA EN INFORMATICA DE GESTIÓ

Memòria treball final



Alumne : Marta Esteve Frigola

Consultor:Cristina Pérez Sola

Juny 2014

Dedicat a Robert

Agraïments a Iolanda per la seva ajuda

Resum

L'objectiu d'aquest projecte és analitzar i desenvolupar una plataforma web existent.

Aquesta plataforma consisteix en un wargame basat amb diferents proves de criptografia .

El projecte comporta l'elaboració de jocs que complementen aquesta plataforma a partir dels diferents algorismes criptogràfics estudiats al llarg del semestre anterior en l'assignatura de criptografia i millorant en la mida del possible el disseny de la mateixa.

Memòria treball final de projecte

1. Introducció....4
1.1 Justificació del TFC i context: punt de partida i aportació del TFC....4
1.2 Objectius....4
1.3 Planificació....5
1.3.1 Diagrama de Gantt corresponent a la planificació inicial....6
1.3.2 Especificació de les tasques....6
1.4 Estat de l'art....7
1.5 Contigut de la memòria....9
2. Elaboració i anàlisi de nous wargames....11
2.1 Quizz de substitució....11
2.2 Quizz de transposició....12
2.3 Quizz relacionat amb criptosistemes de xifres de bloc....14
2.4 Quizz relacionat amb criptosistemes de clau pública....16
2.5 Quizz relacionats amb criptosistemes històrics....18
2.5.1 Esteganografia....18
2.5.2 Màquina Enigma....20
2.5.3 Codi naval japonès....22
3. Elaboració i anàlisi de millores de la plataforma....24
3.1 Afegir un captcha....24
3.2 Crear un nou apartat de links/tutorials i llocs relacionats d'internet....25
3.3 Afegir funcionalitats/ eines d'encriptació....26
3.4 Afegir opcions de multillenguatge....29
4. Proves i validació del producte final....30
4.1 Eines utilitzades....30
4.2 Producte resultant....31
4.3 Validacions....31
5. Conclusions....33
5.1 Diagrama de Gantt corresponent al compliment de la planificació....33
5.2 Anàlisis del compliment....34
6. Apèndix....35
6.1 Manual de instal·lació del servidor en localment....35
6.2 Sil.labari Kana....36
7. Glossari....37
8. Bibliografia....39

1 . Introducció

1.1 Justificació del TFC i context: punt de partida i aportació del TFC

En aquest projecte ens centrarem en crear nous reptes de criptografia , coneguts dins de la comunitat hacker com a **wargames**. Aquests espais web ofereixen diferents reptes a on els usuaris que ho desitgin es registren per començar a resoldre desafiaments . Els més comuns són de tipus criptogràfics, lògica, programació etc ..la dificultat dels quals pot variar.

El projecte parteix d'una plataforma ja existent que primer de tot muntarem en un servidor local. L'objectiu consisteix en ampliar els seus continguts a fi i a efecte d'elaborar nous reptes criptogràfics per tal que els usuaris registrats que així ho desitgin puguin desenvolupar les seves competències.

1.2 Objectius

L'objectiu principal d'aquest projecte consisteix en analitzar ,desenvolupar i complementar una plataforma web existent sobre un servidor web apache amb php.

Aquest, a la vegada el dividirem en dues parts ben diferenciades que consistiran en :

1. Confeccionar nous wargames per incloure nous jocs en base a criptosistemes vistos a l'assignatura de criptografia i també en criptosistemes històrics.

2. Ampliar les funcionalitats operatives de la plataforma.

Seguidament aportem una petita descripció del jocs incorporats i l'algorisme en que es basen :

- Nou quizz de substitució → Xifratge que a partir d'un text en clar cada caràcter es substitueix de forma regular segon la clau establerta .
- Nou quizz de transposició → Xifratge en que els caràcters del text en clar es canvien de posició segons un esquema definit .
- Nou quizz de xifres de bloc → Xifratge que opera en grups de longitud fixa deno-

minats blocs .

- Nou quizz de criptosistema de xifres de clau pública → Xifratge asimètric que utilitza un parell de claus per enviar informació xifrada. Tant l'usuari emissor i receptor disposen d'una clau publica i privada.
- Nous quizzes basats en criptosistemes històrics :
  - Quizz basat en la tècnica d'estenografia
  - Quizz basat en codificació de la màquina enigma
  - Quizz basat en el codi naval japonès

Mencionar també les ampliacions que s'han dut a terme per millorar funcionalitats de la plataforma :

- Afegir un CAPTCHA (*C-ompletely A-utomated P-ublic T-uring Test to tell C-omputers and H-umans A-part*) . Test que ens ajuda a determinar si els usuaris són humans i no màquines. Realitzat tant a l'accés del frontend com al backend.
- Crear un nou apartat de links/tutorials i llocs relacionats d'internet.
- Afegir funcionalitats/ eines d'encriptació.
- Incorporar opcions de multi-llenguatge.

1.3 Planificació

Mostrem a continuació la taula inicial on detalla la planificació del projecte :

ENTREGA	CONTINGUT	INICI	FINAL
PAC 1	Pla de treball	26/02/2014	27/02/2014
PAC 2	Resultat de la fase d'anàlisi i disseny	28/02/2014	14/04/2014
PAC 3	Implementació del problema plantejat	15/04/2014	19/05/2014
PAC 4	Memòria del projecte	20/05/2014	13/06/2014
Presentació virtual	Presentació virtual de la síntesis del projecte.	14/06/2014	20/06/2014

Taula 1 .1 planificació

1.3.1 Diagrama de Gantt corresponent a la planificació inicial

Presentem a continuació el diagrama de proposta inicial en la planificació de la pac1

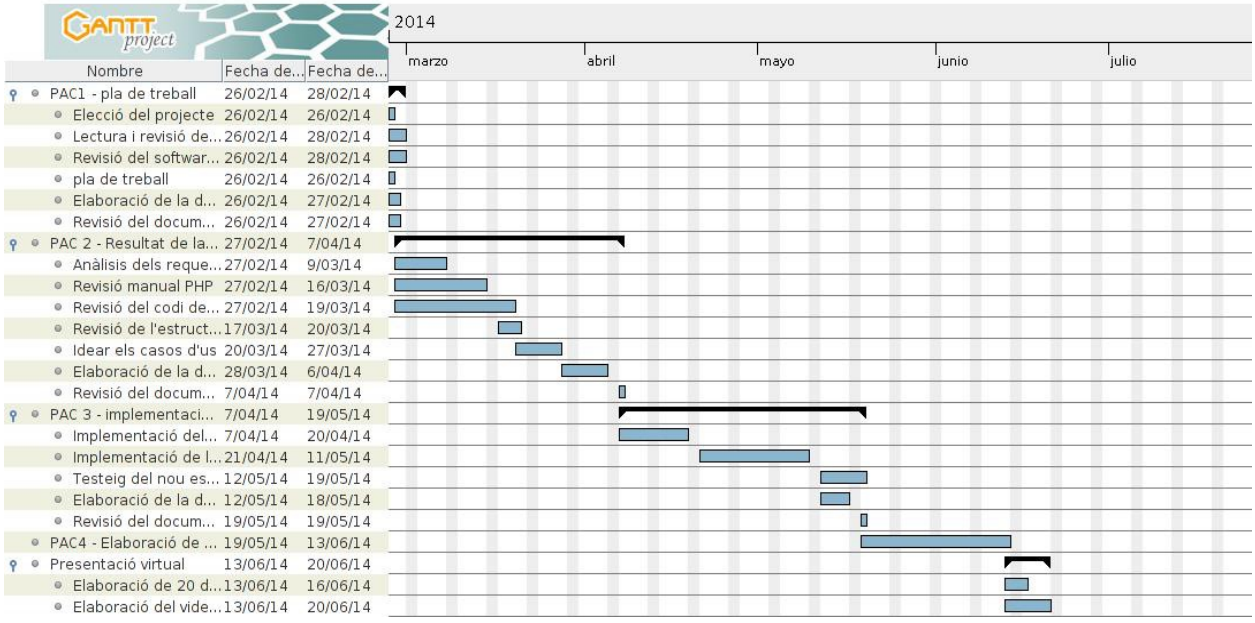


Figura 1.1 Diagrama de Gannt

1.3.2 Especificació de les tasques

Detall de cadascuna de les tasques que s'han realitzat :

1.Elecció del projecte → Seleccionar de les dues propostes de pla docent aquella més adequada als objectius plantejats pel projecte final .

2.Realització de la PAC1 → Definir cada una de les tasques amb una temporalització corresponent en funció dels objectius generals i específics del projecte , del seu mètode i tenint present l'estat de l'art .

3.Muntar el servidor en local → Muntar el servidor web en local per poder treballar en la nova implementació. Instal·lació del software requerit , crear de la base de dades i comprovar la seva funcionalitat.

4.Revisió del codi de la plataforma muntada → Revisió i anàlisi del codi amb php que ha lliurat la consultora per la correcte comprensió del seu funcionament i l'aprofundiment dels coneixements teòrics del llenguatge PHP necessaris pel desenvolupament d'aquesta .

5.Revisió de la base de dades → Revisar l'estructura principal de la base de dades actual i les relacions de les diferents taules.

6.Idear els nous quizzes per a la plataforma → Dissenyar en base els algoritmes criptogràfics existents nous reptes criptogràfics que poguessin enriquir aquesta plataforma

7.Realització de la PAC2 → Descriure les millores proposades amb els casos d'us corresponents i nou disseny.

8.Implementació → Implementació del codi dels nous reptes i millores descrites en l'anterior pac.

9.Test de la nova configuració → Testar els nous quizzess i millores introduïdes a la plataforma . La introducció de les modificacions oportunes fruit del resultat d'aquest .

10.Realització de la PAC3 → Realització de la pac 3 com a resultat de la fase d'anàlisi i implementació

11.Síntesi del treball realitzat durant el semestre → Síntesis de les tasques realitzades i tots el reptes que s'han anat desenvolupant al llarg del semestre.

12.Realització de la PAC4 → Contindrà la memòria del projecte més el producte resultant. Haurem de mirar si hem assolit els objectius proposats en aquest pla de treball.

Les subtasques en algun moment s'han hagut de modificar per adequar-nos a l'objectiu.

1.4 Estat de l'art

Presentem a continuació algunes de plataformes wargames amb un petit resum dels seus continguts i funcionalitats :

www.wechall.net

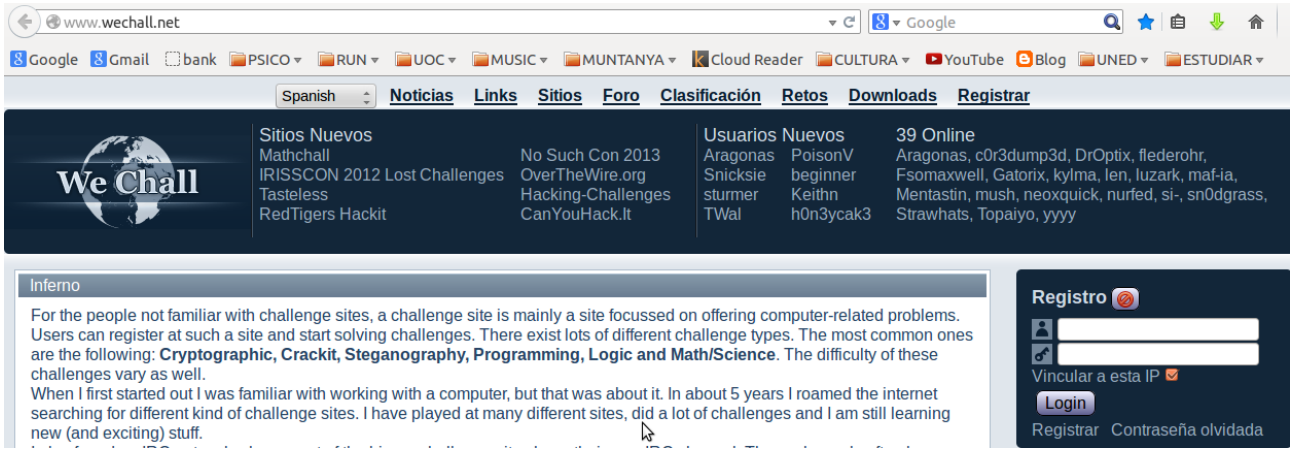


Figura 1.2 We chall

Com es pot veure a la pàgina web es troben links que redirigeixen a nous jocs amb reptes de diferent dificultat segons la tipologia escollida.

Trobem, per exemple, una secció que proporciona 54 links actius d'altres pàgines dedicades als wargames .

http://www.dareyourmind.net/menu.php

Figura 1.3 Dare your mind

En aquesta pàgina hi ha 44 reptes criptogràfics plantejats de menor a major complexitat .

Per a cada un dels reptes existeix un enllaç d'ajuda que proporciona preguntes i respostes d'un fòrum intern.

El propietari de la pàgina no obstant no l' actualitza des de l'any 2012 .

http://www.bright-shadows.net/

Figura 1.4 Bright Shadows

Aquí també trobem una pàgina amb més quantitat de reptes de cada un dels diferents de programació, Java , PHP i criptografia.

Així trobem un apartat de links i eines molt útils per poder comprendre la base teòrica del algoritmes i llenguatges de programació.

1.5 Contigut de la memòria

A continuació en el capítol 2 hi trobarem la descripció detallada dels wargames que s'han agregat a la plataforma especificant els criptosistemes i la forma de resoldre els quizzes. Després el capítol 3 incorpora les especificacions de les noves millores afegides a la plataforma i les diferents tasques realitzades.

El capítol 4 contindrà el producte final i les proves realitzades. Finalment, el capítol 5 recull les conclusions assolides durant el projecte i les possibles línies de treball futur.

2 . Elaboració i anàlisi de nous wargames

2.1 Quizz de substitució

Descripció del criptosistema :

Com a primer quizz introductori s'ha inclòs un wargame basat amb xifra de substitució com el de Cèsar. Aquests criptosistemes substitueixen una lletra de text en clar per una altra a una distancia fixa de posicions de l'alfabet que anomenem clau.

Descripció dels atacs coneguts :

Els criptosistemes basats en substitució simple són dels més senzills. El criptoanàlisis es pot realitzar força ràpid ja que moltes vegades a simple vista es pot deduir el text pla directament amb el tros de codi interceptat.

Si disposem només del text encriptat sense saber exactament quina es la distància utilitzada podem desxifrar-lo fàcilment utilitzant els següents mètodes :

- Anàlisi de freqüències - Com que aquest criptosistema no amaga les freqüències de les diferents lletres del text original només hauríem de tardar 25 caràcters per poder deduir el text en clar.
- Atac de força bruta - També es pot utilitzar un atac de força bruta provant totes les possibles distancies una a una . Si realitzem l'encriptació amb l'alfabet de 26 caràcters obtenim 25 possibles solucions.

Descripció del quizz :

El primer wargame que proposem s'anomena *missage intercepted*. El joc esta basat en un algoritme de substitució però en comptes d'utilitzar l'alfabet utilitzem el codi ASCII .

L'usuari haurà d'esbrinar que es tracta d'un sistema de substitució però no directament el de Cèsar sinó que hi ha una transformació prèvia a ASCII.

Com a eina addicional a la plataforma s'ha inclòs una eina per encriptar text amb el criptosistema de Cèsar amb un alfabet de 25 i també amb codi ASCII.

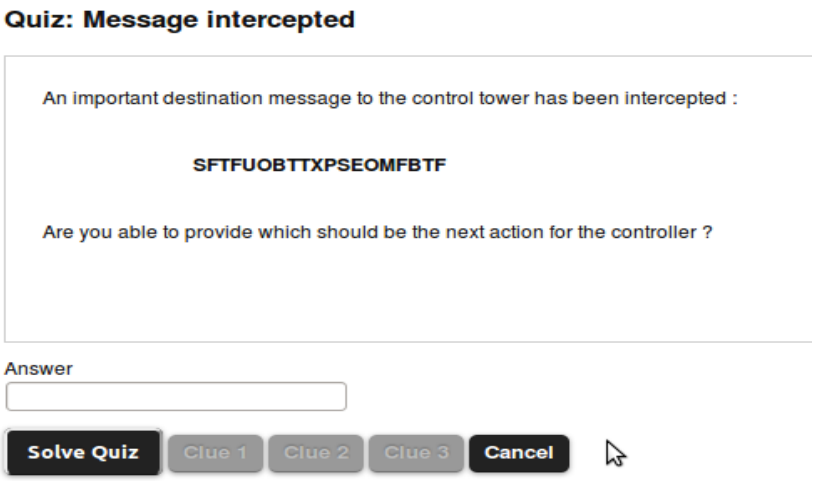


Figura 2.1 Message intercepted

Solució del quizz	Pistes aportades
RESET THE PASSWORD PLEASE	Indicar que es tracta d'un criptosistema de substitució. Mirar el tutorial per a més informació
	Indicar la paraula clau ASCII per fer entendre que hi ha una transformació prèvia amb aquest codi
	Convidar el jugador que utilitzi l'apartat d'eines de la plataforma

Taula 2.1

2.2 Quizz de transposició

Descripció del criptosistema :

Els criptosistemes basats en algoritmes de transposició consisteixen en reordenar els caràcters del text en clar amb unes certes regles .

Hi ha casos que ens trobem amb criptosistemes de simple de transposició que funcionen partint el text en en blocs de la mateixa mida (període) . Per la divisió s'utilitza una clau la mida de la qual serà el període i ens indicarà la distancia de la permutació de cada membre del bloc.

Descripció dels atacs coneguts :

Per realitzar la criptoanàlisi sabem del cert que el missatge encriptat conté els mateixos caràcters continguts en el text en clar transposats en un determinat període.

Els criptosistemes de transposició es poden trencar per mitja d'atacs de força bruta però hi ha un inconvenient amb això ja que suposa un elevat grau de complexitat. En el cas que la clau sigui molt llarga el nombre de permutacions augmenta considerablement. Si per exemple haguéssim de testejar totes les possibles combinacions fins una clau amb una llargada de 6 lletres seria aproximadament fàcil (son unes 720 possibilitats) però a mesura que augmentem la mida de la clau els càlculs son insostenibles.

Una possibilitat per tal de disminuir el temps de càlcul consistiria l'ús de diccionaris ja que partim de la hipòtesis que la paraula usada es una existent.

El segon wargame seria un simple missatge amb una transposició simple amb una clau de 4 dígits. El missatge es podria trencar intentant transposar blocs del text de diferent llargada .

Descripció del quizz :

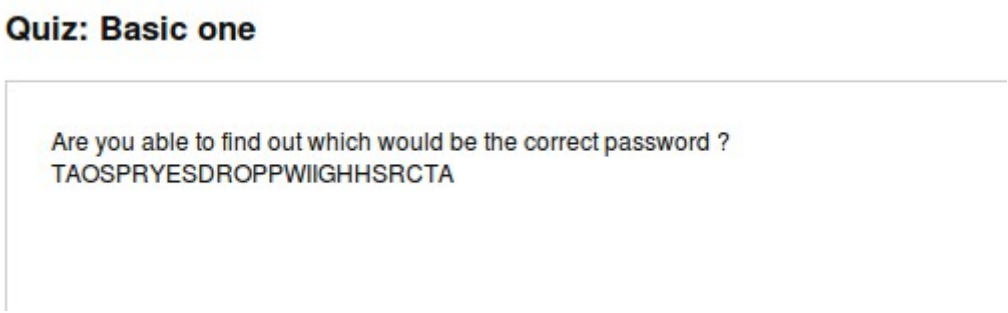


Figura 2.2 Basic one.

Solució del quizz	Pistes aportades
CRIPTOGRAPHY	Indicar que es tracta d'un criptosistema de transposició
	Indicar la mida de la clau
	Indicar la clau mateixa que és tracta de la paraula CODE.

Taula 2.2

2.3 Quizz relacionat amb criptosistemes de xifres de bloc

Descripció del criptosistema :

DES es un criptosistema de xifratge de bloc que encripta el text en clar en blocs de 64 bits. Utilitza una clau de 56 bits. El mateix algoritme i clau són utilitzats tant per encriptar com per desencriptar i per tant tota la seguretat del criptosistema es basa en la clau.

Les tècniques utilitzades per construir el bloc es componen d'una combinació de substitució seguit d'una permutació basat en la clau. Tot aquest procés es desencadena durant 16 repeticions. Amb DES es possible utilitzar la mateixa funció per encriptar i per desencriptar amb la diferencia que les claus s'han d'utilitzar en ordre invers.

Hi ha diferents modes d'operar que són ECB,CBC,OFB i CFB.

Descripció dels atacs coneguts :

Els atacs més usuals que es realitzen amb aquest criptosistema són els atacs de força bruta . No obstant també existeixen diferents atacs teòrics possibles però portats a la pràctica són més complexes i requereixen de més temps que un atac de força bruta .

Descripció del quizz :

Com a quizz plantegem un text xifrat amb DES i el mètode CBC. Es presenta text xifrat amb la clau corresponent .

Quiz: A poem

The first 4 verses of a poem have been sent encripted :

f4a0d3d3deb56bdfd9ee3c2924ff7684
27c39180766e5a12547003426dc99334
e2a95486def4cf1497178bc9ed02d854
12105dafe2310edd2ba088519a8d2fc4
ab67408b60e0d64[illegible]a78207d358d23ef5
f52ba78fff9d6d048569a392bbd8c9e8
26ee910dfba1bdea07ed68f1a9811eec
395c2307246879ada9fba75749d893f5
59d91cfb24a1782b5467b0c243b5477f
2c454e8daabb32ec0d5a75526889fa95

We only have found out that the key is -> FRGH

Figura 2.3 A poem

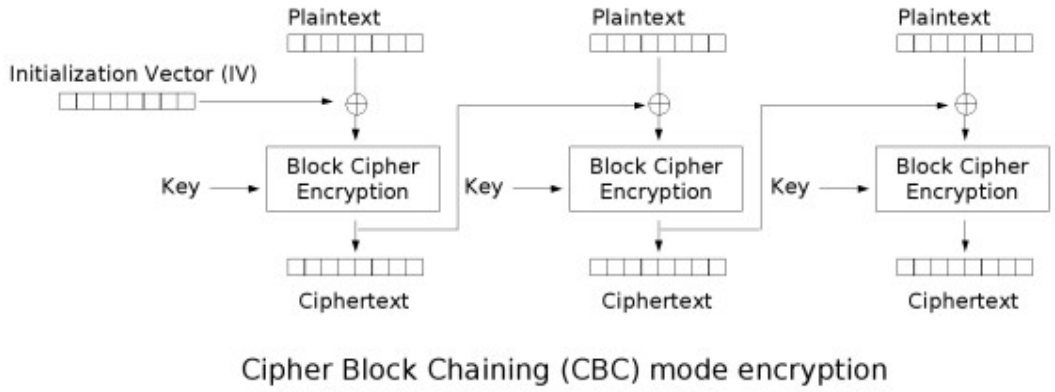


Figura 2.4 CBC

Solució del quizz	Pistes aportades
La solució del quizz es un poema anomenat **A FUNERAL ELEGY** atribuït a William Shakespeare ja que qui firmava el poema era amb les inicials WS.	Indicar que el text està encriptat en un criptosistema de xifra de bloc
	Presentar el mode d'operació del criptosistema que és CBC
	Mostrar el vector inicial

Taula 2.3

2.4 Quizz relacionat amb criptosistemes de clau pública

Descripció del criptosistema :

Un dels criptosistemes més populars és el **RSA** . El mètode d'encriptació de RSA està basat en propietats de l'aritmètica modular i en la dificultat de factoritzar nombres grans en nombres primers. La majoria de criptosistemes de clau pública estan basats en aquest principi.

Descripció dels atacs coneguts :

Per poder trencar aquest criptosistema s'ha de poder conèixer el valor φ(n) a partir de n i això implicar factoritzar aquest nombre n en dos nombres primers pi q . El que interessa es que la factorització sigui el mes difícil possible. Normalment s'escolleixen els dos primers de forma aleatòria. Si el nombre no es molt gran es pot trencar fàcilment però ara be la dificultat augmenta considerablement amb nombres suficientment llargs.

Resumim aquí en una taula les claus que intervenen en el criptosistema RSA :

Clau pública	N es producte de dos nombres primers p y q i e que ha de ser primer relatiu a (p-1)(q-1)
Clau privada	$(d, e^{-1} \bmod ((p - 1)(q - 1))$
Encriptació	$c = m^e \bmod n$
Des encriptació	$m = c^d \bmod n$

Taula 2.4

Factoritzar nombres llargs és una àrdua tasca encara que ha evolucionat molt durant els últims anys. De totes maneres com més llarga sigui la clau més temps de computació es necessita per tant l'ideal es que la clau sigui el suficientment llarga perquè sigui segura i suficientment curta perquè l'encriptació tardi un temps raonable.

Descripció del quizz :

Com a primer quizz introductori s'ha proporcionat N el qual s'ha de descompondre en p i q

Un primer quizz de RSA bàsic :

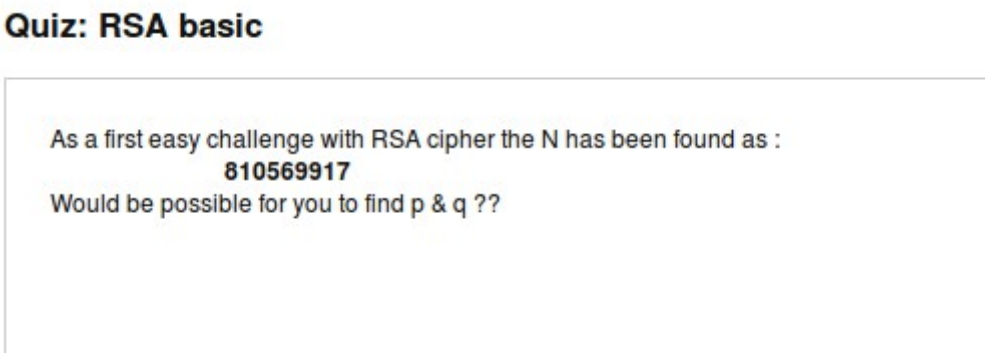


Figura 2.5 RSA basic.

Solució del quizz	Pistes aportades
25537*31741 Hem de factoritzar N per tal de poder trobar p i q. Com que el nombre N no conté molts dígits es podria realitzar fàcilment amb qualsevol calculadora online.	Indicar que N és el resultat de multiplicar dos nombres primers
	Indicar que existeixen gran varietat de calculadores de factorització

Taula 2.5

Descripció del segon quizz de RSA :

Hem introduït també un nou repte de més dificultat amb molts més dígits de RSA. En aquest challenge proporcionem el codi encriptat i la clau pública formada per la parella de nombres N i e.

L'encriptació funciona de tal forma que els divideix en blocs de dos caràcters el text en clar . Seguidament transformem el dos caràcters en codi ASCII i posteriorment a binari obtenint blocs de 23 dígits.

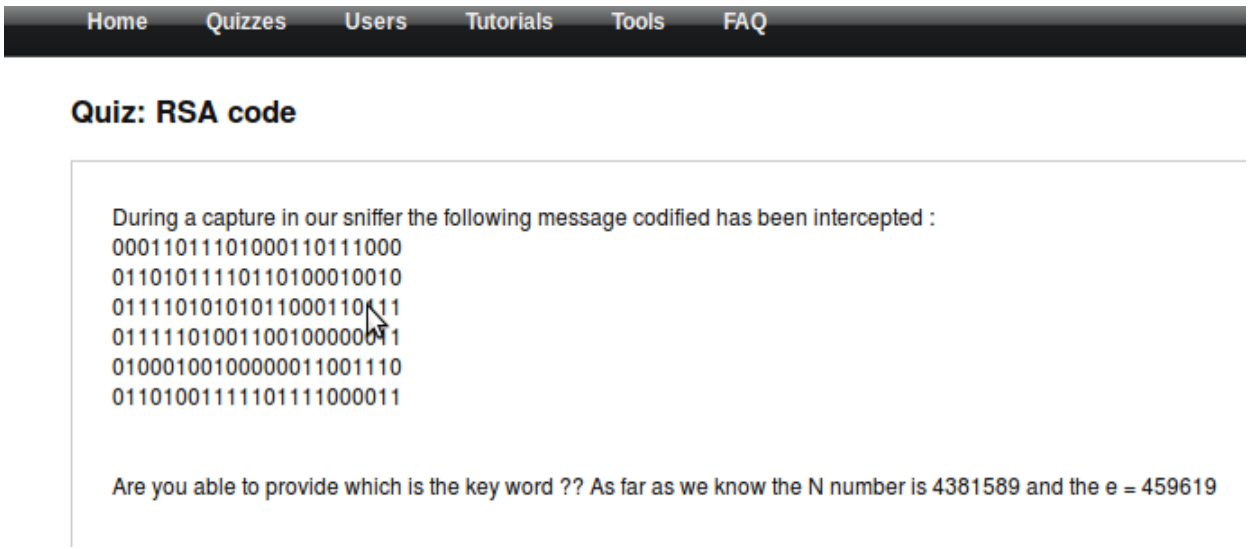


Figura 2.6 RSA code

Solució del quizz	Pistes aportades
La solució del quizz correspon a la paraula CRIPTOGRAFIA	Indicar que el primer pas es la factorització de N
	Destacar la transformació prèvia dels caràcters a codi ASCII
	Indicar la utilitat d'una eina de càlcul RSA online

Taula 2.6

2.5 Quizz relacionats amb criptosistemes històrics.

2.5.1 Esteganografia

Descripció del criptosistema :

Sir Francis Bacon va desenvolupar un mètode per poder codificar missatges secrets de forma que a primera vista no es percep com un missatge en el cas d'un observador que no conegui la seva existència . Aquesta es la ciència que es coneix amb el nom d'esteganografia la qual estudia les tècniques d'ocultació de missatges dins d'altres objectes .

Cada caràcter del text en clar es codifica amb una paraula de 5 lletres que només conté els caràcters a i b. La mostrem a continuació :

	Code		Code		Code
A	aaaaa	I/J	abaaa	R	baaaa
B	aaaab	K	abaab	S	baaab
C	aaaba	L	ababa	T	baaba
D	aaabb	M	ababb	U/V	baabb
E	aabaa	N	abbaa	W	babaa
F	aabab	O	abbab	X	babab
G	aabba	P	abbba	Y	babba
H	aabbb	Q	abbbb	Z	babbb

Taula 2.7

Descripció dels atacs coneguts :

Si es coneix el principi sobre el que es basa el criptosistema ja no hi ha seguretat. L´objectiu d'aquest mètode precisament es amagar el fet sobre el qual es basa.

Descripció del quizz :

El quizz plantejat es basa en aquesta tècnica diferenciant majúscules i minúscules de la codificació de a i b.

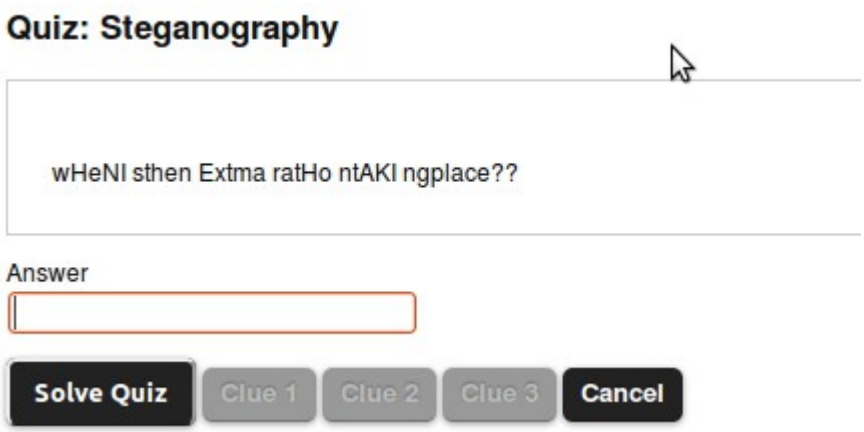


Figura 2.7 Steganography

Solució del quizz	Pistes aportades
La paraula es MARCH	Indicar que el secret del missatge s'amaga en el missatge en si
	Mencionar el nom de Francis Bacon
	Denotar que que les majúsculs son la lletra b .

Taula 2.8

2.5.2 Màquina Enigma

Enigma era el nom de la màquina electromecànica utilitzada pels alemanys durant el transcurs de la segona guerra mundial per xifrar els missatges que s'intercanvien les tropes de terra.

La màquina consistia en un teclat a on s'introduïa el tex en clar i interiorment hi havien tres rotors (que s'escollien d'un total de 5) i un teclat d'interconnexió al front. La font era subministrada per una bateria instal·lada dins la màquina i així d'aquesta forma es podria mostrar la lletra codificada amb una senyal l lumínica.

Els rotors mecànics funcionaven de tal forma que primer girava el primer fins que en esgotar les posicions i aquest feia girar el segon i de la mateixa forma el tercer. Hi havia un rotor ràpid, mitja i lent per dir-ho d'alguna forma .

Figura 2.8 Màquina enigma

Addicionalment als rotors alguns models incloïen un teclat frontal (Steckerbrett) d'interconnexió similar a les velles centraletes telefòniques. Dels 26 possibles caràcters de l'alfabet interconnectava 20 lletres en 10 parells .

Figura 2.9 Steckerbrett

Per poder codificar i descodificar els missatges tant l'emissor com el receptor necessitaven posicionar els rotors inicials de la màquina de la mateixa forma . Aquestes posicions es notificaven en una taula que canviava cada dia del mes. Els alemanys transmetien per ràdio o per paper aquest codis. En el cas que es produís la situació d'interceptar aquest codi amb l'ajuda d'una maquina Engima exacta es podia descodificar el codi directament.

El factor clau perquè els britànics poguessin trencar les comunicacions interceptades amb la màquina enigma va ser que la lletra codificada mai es coincidiria amb ella mateixa és a dir si per exemple es premia la lletra A del teclat totes les llums en el panell es podien il·luminar excepte la lletra mateixa. Gràcies a aquest descobriment va permetre els anglesos fabricar la *Bomb machine* amb la qual es podia descodificar els missatges amb un temps molt més ràpid.

Descripció del quizz :

El quizz plantejat l'he anomenat Bletchley Park que el centre d'operacions que van establir els anglesos durant la segona guerra mundial. Es tracta de descodificar text interceptat de la maquina Enigma. Per poder desxifrar-lo és important saber la posició dels rotors inicials . Aquesta informació es proporciona com a pista.

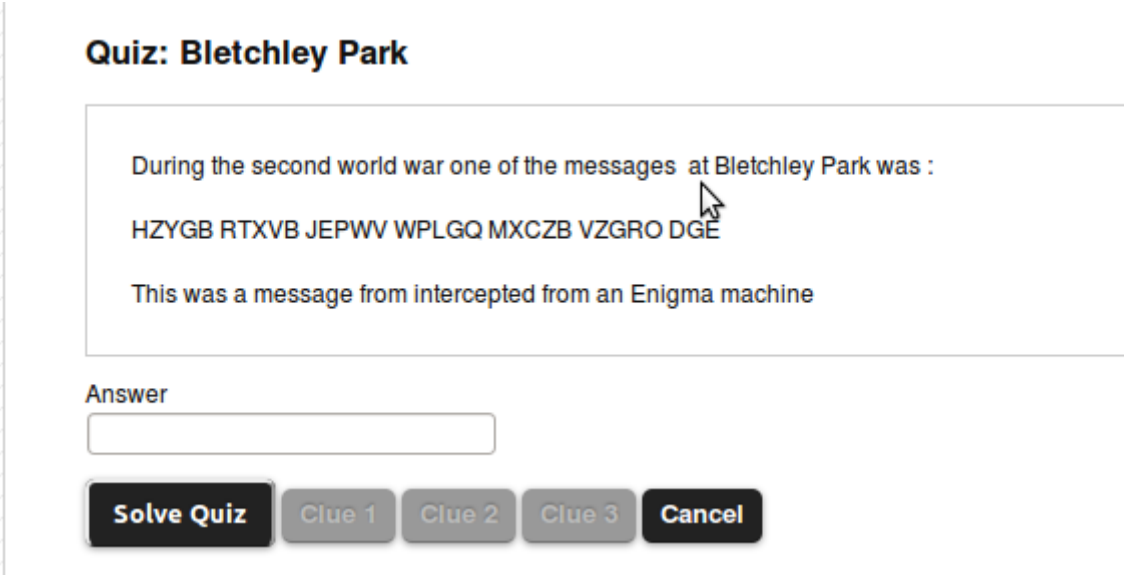


Figura 2.10 Bletchley Park

Solució del quizz	Pistes aportades
Consisteix en la frase IT WAS THANKS TO THE ULTRA THAT WE WON THE WAR	Indicar la posició inicial dels rotors . Pista indispensable per poder desxifrar el codi a menys que utilitzem les tècniques de la bomb machine
	Indicar el tipus de rotor – B
	Indicar que el Steckerbrett en aquest cas no estava connectat.

Taula 2.9

2.5.3 Codi naval japonès

Durant la primera guerra mundial l'armada japonesa va introduir un codi xifrat no per una màquina com l'Enigma sinó de forma manual . Aquest sistema consistia en un diccionari de 33333 lletres paraules i frases les quals tenien assignades un nombre de 5 dígits. Totes les paraules que no estaven incloses en el diccionari s'escrivien en kana . La segona part del xifratge consistia en una taula sumatòria numerada amb nombres aleatoris en línies i columnes també identificades amb nombres. Cada sis mesos es modificava aquesta taula .

Al tractar-se d'un mètode manual i també tinguen en compte que es van interceptar un gran nombre de missatges es va poder desxifrar el codi bastant-se en patrons de conducta més els error per la transmissió de radio.

Com a últim quizz proposo un missatge amb codi Morse utilitzant el sil·labari kana .

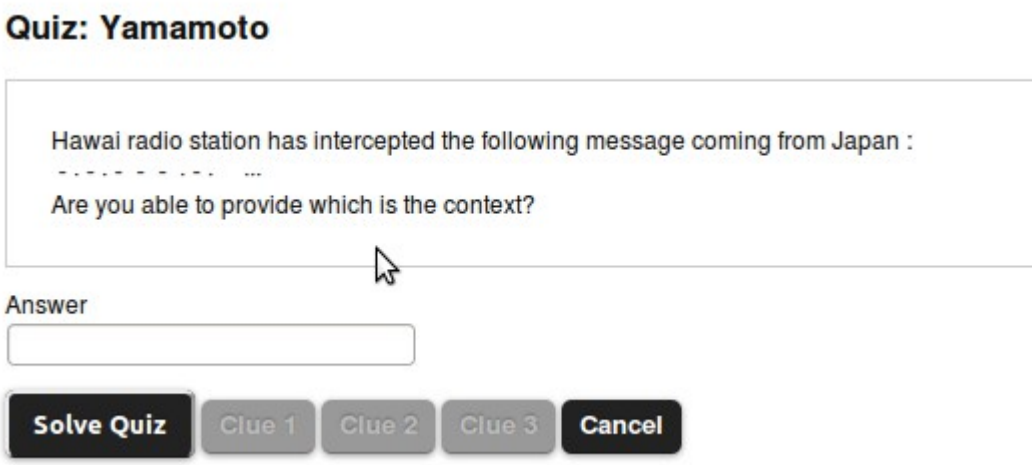


Figura 2.11 Yamamoto

Solució del quizz	Pistes aportades
sayonara	Indicar que codi interceptat es morse code
	Indicar com a pista el poema iroha ja que utilitza cada un dels caràcters del sil·labari kana
	Indicar la paraula clau kata-kana que es un dels dos sil·labaris empleats en l'escriptura japonesa.

Taula 2.10

3 . Elaboració i anàlisi de millores de la plataforma.

3.1 Afegir un captcha

Com a mesura de seguretat hem afegit un **CAPTCHA** (*Completely Automated Public Turing test to tell Computers and Humans Apart)* per accedir tant en el login de frontend com el backend.

Aquest test consisteix en un sistema de reconeixement que s'utilitza per determinar si l'usuari que accedeix a l'aplicació es humà o una màquina que processa les dades de forma automàtica. S'utilitzen formularis i el més comú es que sigui mitjançant una imatge que es mostra que contingui ja sigui lletres o nombres . Les imatges deformades son difícils de llegir per màquines en canvi un humà les pot entendre fàcilment.

Hem utilitzat la llibreria existent reCAPTCHA i per tant hem hagut de descarregar la llibreria i incloure-la dins del nostre codi font de la plataforma → recaptchalib.php

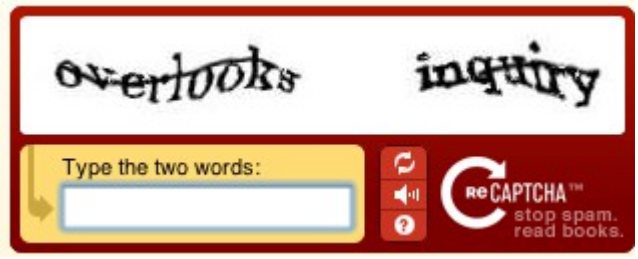


Figura 3.1 reCaptcha

En aquest cas hem d'obtenir una clau publica(Per els usuaris finals de la pagina) i privada (utilitzada per la comunicació entre el servidor i el servidor de reCaptcha) pel nostre domini. Com que el servidor s'ha muntat localment només ens servirà per localhost . En el cas que tinguéssim més d'un domini s'haurien de crear un nou parell de claus.

Els diferents reptes que hem agut d'afrontar per la plataforma existent son :

- Determinar en quina part del codi de la plataforma hem hagut d'incloure la llibreria , modificar els arxius index.php tant del frontend com del backend i finalment incloure en els templates html la part del captcha .
- Afegir un nou filtre per Twig.

3.2 Crear un nou apartat de links/tutorials i llocs relacionats d'internet

Per tal de complementar la pàgina he afegit links a diferents tutorials dels principals algoritmes que es tracten en els quizzes plantejats. També s'inclou links a simuladors existents que son molt útils a l'hora de encriptar o desencriptar alguns criptosistemes :

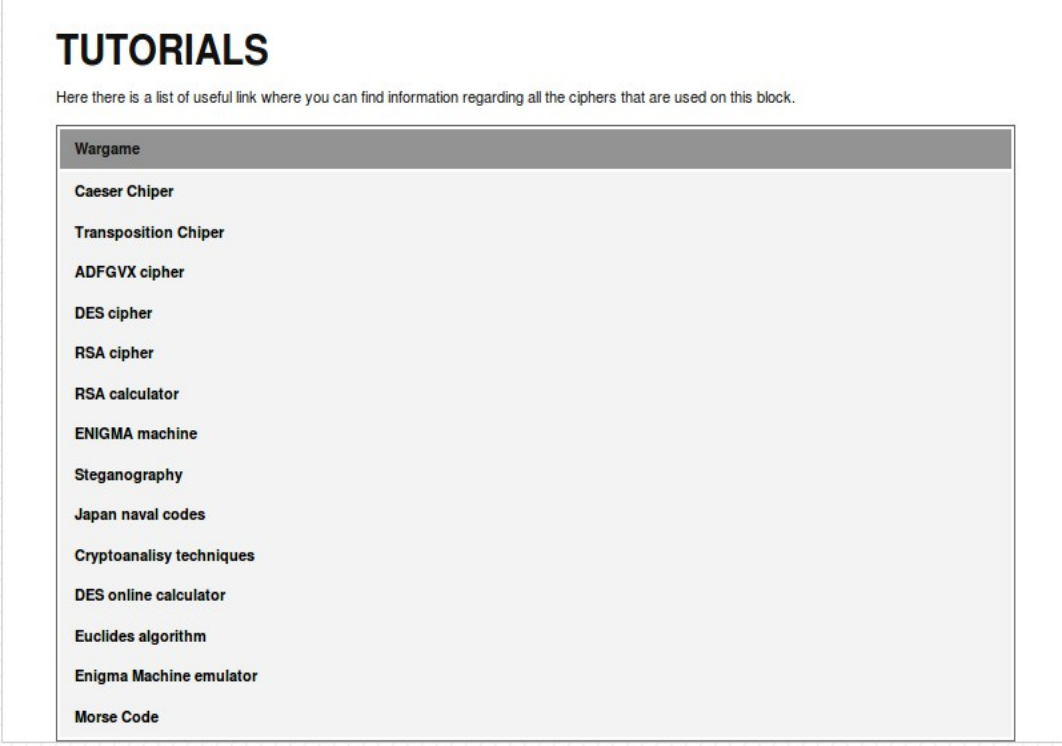


Figura 3.2 Tutorials

3.3 Afegir funcionalitats/ eines d'encriptació

Com a mesura addicional a la la plataforma s'han agregat diferents eines per poder encriptar/desencriptar text en clar. Per poder realitzar-ho hem utilitzat alguns dels algoritmes emprats en la realització dels quizzes .

S'ha creat una nova classe ***Caesar*** per poder codificar/descodificar text en clar. Aquest classe consta de 2 funcions per realitzar la codificació amb un alfabet de 26 caràcters i dos funcions complementaries que realitzen una segona opció amb la conversió de codi ASCII.

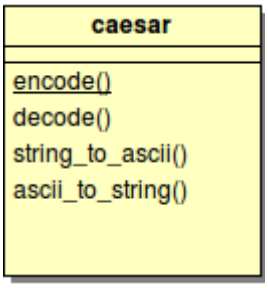


Figura 3.3 Caesar

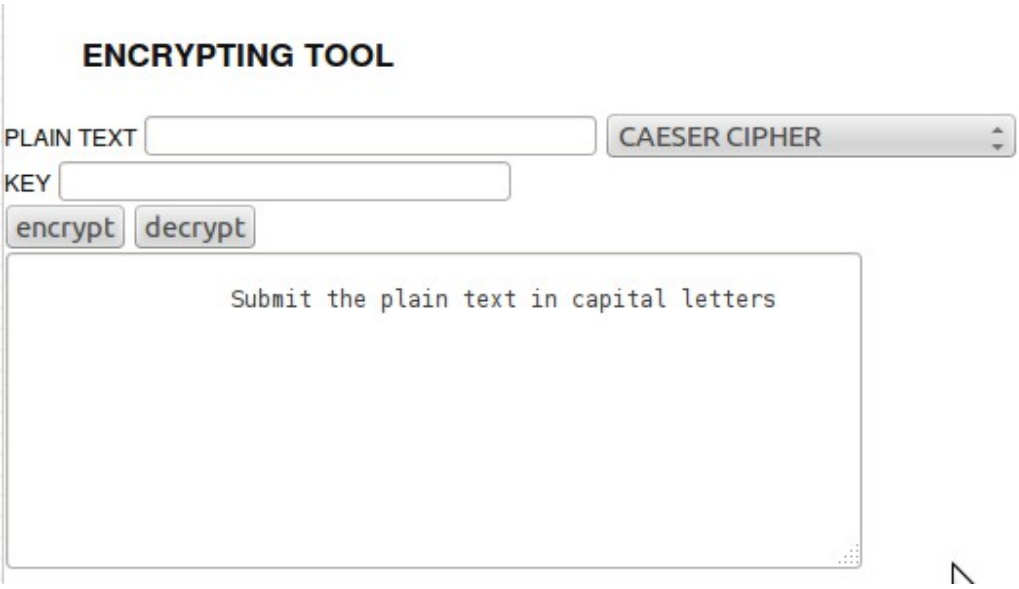


Figura 3.4 Encrypting tool

Com a mesura suplementaria també s'ha utilitzat la llibreria **phpseclib** que esta llicenciada per la *MIT_License* per tant es una llibreria completament lliure .

Aquesta llibreria ens permet realitzar el següent

- Diferents operacions amb enters grans.
- RSA
- SSH2
- SFTP
- X.509
- Algoritmes d'encriptació de clau simètrica com : Rijndael, Twofish, Blowfish, DES,3DES ,RC4 i RC2 .

Per poder emprar aquesta llibreria s'ha creat la classe rsa1 localitzada a public/lib/phseclib/rsa1.php fent ús de les funcions de la llibreria RSA.php.

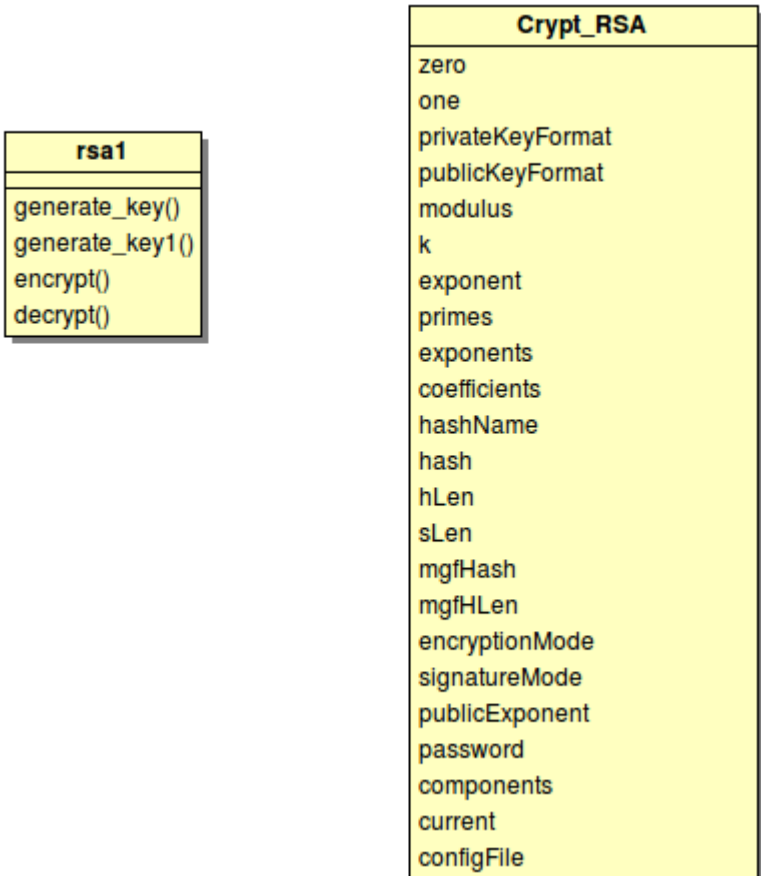


Figura 3.5 rsa1

En l'apartat de eines podem generar claus publiques i privades amb el format PKCS#1.

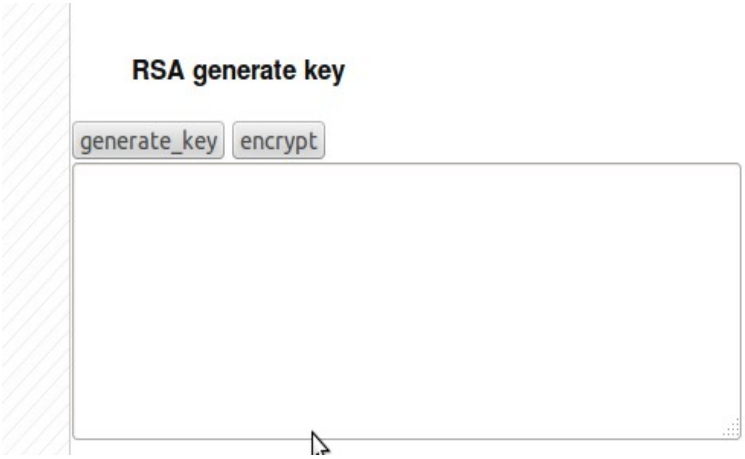


Figura 3.6 RSA generar la clau

I també encriptar i desencriptar amb RSA amb mode PKCS#1:

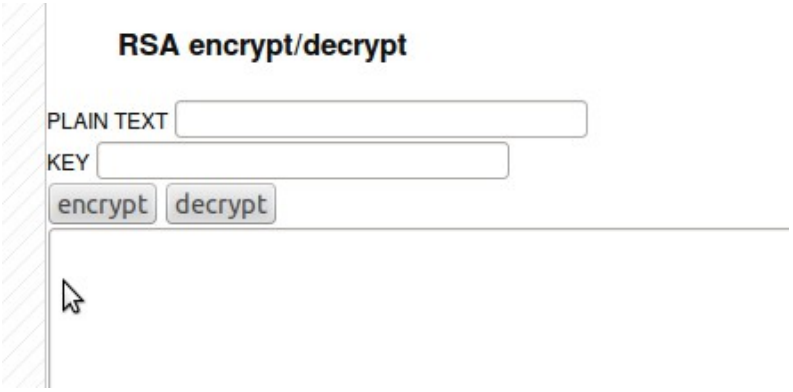


Figura 3.7 RSA encriptar/desencriptar

Com a possibles millora es podria implementar diferents eines per tots els diferents algoritmes d'encriptació que suporta la llibreria.

3.4 Afegir opcions de multillenguatge

Per poder internacionalitzar la pàgina hem hagut de descarregar un extensió del motor de plantilles de Twig ja que aquest no la inclou per defecte . Aquesta extensió l'hem hagut d'incorporar dins de les Extensions de Twig.

L'extensió corresponent és la i18.n la qual permet implementar gettext del llenguatge php. Les funcions de gettext corresponen a un conjunt d'utilitats que formen part del projecte GNU i faciliten la traducció de programes.

El llenguatge per defecte s'entén que es tot en anglès i en el codi font indiquem es el llenguatge que s'ha d'utilitzar .

S'han realitzat les següents tasques :

- Creació dels arxius dels diferents idiomes a través de Poedit. S'han desat a la ubicació /public/locale
- Originar els diferents arxius amb extensió po per cada un dels idiomes de la pàgina
- Configurar els paràmetres de domini i la ruta als paràmetres de la traducció.
- Crear un array en textos_layout.php que després poedit ens ajudarà a traduir.

Figura 3.8 Home page en castella

4 . Proves i validació del producte final

4.1 Eines utilitzades

Durant el desenvolupament del projecte s'ha instal·lat el servidor en local amb un SO Linux Ubuntu.

S'han emprat les següents versions de programari :

XAMPP per Linux 1.8.3-1

XAMPP és una distribució d'Apache completament gratuïta que conté MySQL , PHP i PERL.

PHP version 5.5.3

És un llenguatge de codi obert orientat al desenvolupament web que pot ser incrustat en HTML. La gran avantatge de PH es que el codi s'executa en el servidor i d'aquesta forma el HTLM generat s'envia al client . Aquest no tindrà accés al codi font del mateix.

Apache 2.0

Servidor web de codi obert. Actualment és un dels més utilitzats.

Mysql 5.0.11

Sistema de gestió de bases de dades relacionals de codi obert molt estès.

Twig

Es tracta d'un motor de plantilles lliure per el llenguatge PHP. Per tal de que funcioni correctament es necessita una versió de PHP superior a la **5.2.4** .

Eclipse for PHP Developers

Paquet dins del IDE Eclipse pel desenvolupament de php.

BOUML 4.21

Eina per realitzar diagrames UML i el més útil es que proporciona enginyeria inversa ja que a partir de codi font crea els diagrames i documentació corresponent .

Poedit 1.4.6

Poedit es un programa lliure i gratuït que permet editar els arxius amb extensió .PO. Aquest arxius ens permeten la traducció a altres idiomes.

4.2 Producte resultant

Una carpeta public amb tota la codificació :

public – amb tots els arxius *.php

/templates – Conté tots els templates html del frontend

/doc- Carpeta que conté tota la documentació html de generat amb **BOULM**

/locale- Arxius de la plataforma multi llenguatge.

/lib – Conté llibreries entre elles Twig i la nova afegida phpseclib

/img- Imatges utilitzades

/admin- Conté tota la codificació del backend

/config – Arxius de configuració de la instal·lació. Per a més informació veure l'arxiu README de la private folder

/avatar – imatges dels avatars.

/css – Especificacions css.

Una carpeta private amb

Readme.txt- Arxiu a on s'explica el procediment d'instal·lació

/script – Carpeta que conté l'script amb els usuaris i els quizzes .

4.3 Validacions

Tas-ca	Nom	Descripció	Observacions	Resultat	Accions realitza-des i possibles futures
1	Registrar-se	Registrar-se a la plataforma amb un nou correu electrònic.	El mail arriba correcta-ment. Al tractar-se d'un servidor en local en el link de confirmació apa-reix el port 8888 . Si es treu del link la confirma-ció es correcta.	Majoritàriament satisfactòria .	Modificació de l'ar-xiu config.ph l'a-partat $BASE_URL
2	Login	Login al fron-tend amb usuari password i capt-cha	S'ha introduït la informa-ció correcta	Esperat	
3	Login	Login al bac-	S'ha introduït la informa-	Esperat	

		kend amb admin/admin i captcha	ció correcta		
4	Login	Login al frontend amb usuari i password sense captcha	Torna a aparèixer la pantalla de login	Esperat	Incloure un missatge d'error de captcha
5	Login	Login al backend amb usuari i sense captcha .	Ok apareix arror amb access denied	Esperat	
6	Quizzes	Mostrar els quizzes de nivell 1 o nivell 2 segons el perfil de l'usuari	Ok provat amb diferents usuaris amb diferents nivells aconseguits	Esperat	
7	Quizzes clues	Mostrar les diferents pistes dels quizzes	Amb les pistes disponibles 3 podem visualitzarles	Esperat	Possibilitat d'aconseguir més pistes a mesura que es van aconseguint punts . Possibilitat de modificar el nombre de pistes en el backend.
8	Tutorials	Funcionament dels links dels tutorials	Els links funcionen correctament	Esperat	
9	Eines	Ceaser	Encriptació / Des encriptació de l'eina amb Ceaser.	Esperat encara que només funciona amb majúscules	Possibilitat de diferenciar entre majúscules i minúscules.
10	Eines	RSA	Generar clau i encriptació correcta sempre que sigui amb la clau que hagim generat	Esperat	Incloure els algoritmes DES, Rjndael etcc..
11	Llenguatge	Espanyol	Traducció de la pàgina al espanyol	Esperat en les parts que s'han passat al l'arxiu text:layout	El backend i els quizzes segueix apareixent amb angles . Els quizzes ja que ataquen directament a la base de dades.

Taula 4

5 . Conclusions

En ser una plataforma ja muntada malgrat pogués semblar a priori més fàcil trobo que per la meva part ha resultat més complexe de l'esperat sobretot la part de programació en php i programació en twig .

Aquesta pràctica ha resultat per tant molt útil per l'assoliment de de competències del llenguatge de desenvolupament web php amb plantilles basades en Twig per una banda i per altra la millor comprensió del criptoanàlisi d'alguns algoritmes .

També ha m'ha servit per aprendre a com estructurar, elaborar i sintetitzar un text científic.

Aquesta es una primera aproximació de millora de la pàgina. Per a futures versions es podrien incloure mes eines de xifratge i també mes reptes per donar més joc a la plataforma .

5.1 Diagrama de Gantt corresponent al compliment de la planificació

Presentem el diagrama modificat i amb vermell destaquem la part no complerta en dates de la planificació inicial.

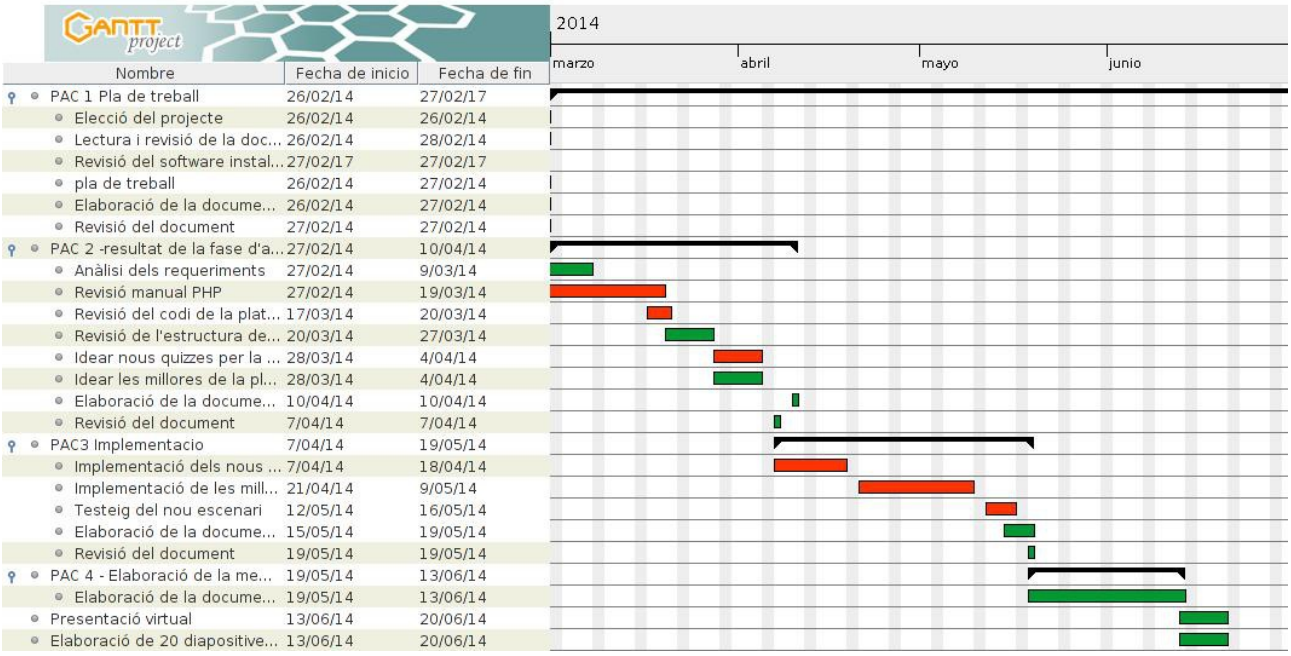


Figura 5.1 Diagrama de Gantt

5.2 Anàlisis del compliment

Analitzem les tasques que realment han portat més temps que l'esperat

- Revisió manual PHP- Tot i ser un llenguatge d'alt nivell m'ha dut més temps que l'esperat entendre bé el funcionament
- Revisió codi de la plataforma- Revisar tot el codi de la plataforma , estructura i anàlisis m'ha portat més temps del previst . Sobretot en la part de comunicació de pas de paràmetres entre twig y php.
- Idear quizzes y millores. Per tal de realitzar els quizzes vaig inspirar-me en l'estat de l'art i en la lectura d'alguns llibres mencionats en la bibliografia. Tot aquesta recerca em va portar a estar més temps que l' inicialment previst en el pla de treball.

Addicionalment analitzem el que no s'ha pogut dur a terme :

- Creació d'un fòrum – No s'ha pogut programar ja que per falta de temps al final en la programació
- Opcions de multi llenguatge- Acabar amb la traducció de totes les pagines i afegir l'idioma català i Alemany.

6 . Apèndix

6.1 Manual de instal·lació del servidor en localment

Per poder instal·lar el servidor en local com a recomanació es podria utilitzar XAMPP que es l'entorn de desenvolupament PHP més popular ja sigui per sistemes operatius Windows com per Linux.

Un com hem instal·lat el programari hem d'executar Apache amb Mysql i assegurar-nos que s'està executant correctament a través de localhost :

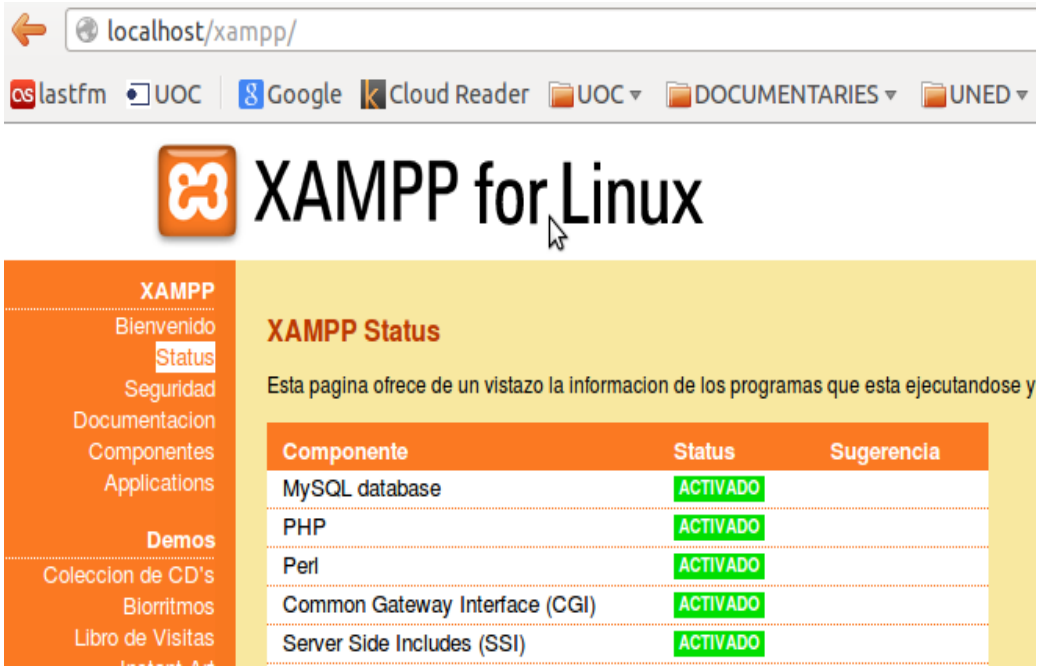


Figura 6.1 XAMPP

Per poder prosseguir haurem de realitzar un primer pas que es tracta de configurar l'arxiu config.php que es troba a dins **/config**

// BASE DE DADES :

$DATABASE_HOST = 'localhost'; - Aquí hem d'introduir localhost en el cas que estem treballant en local .
$DATABASE_USER = // Usuari de la base de dades
$DATABASE_PASS= // password de la base de dades
$DATABASE_NAME = // Nom de la base de dades

Copiar tot el contingut de la carpeta public a on volem desplegar el servidor. En el cas

del Xampp correspon a → **/opt/lampp/htdocs**

Un cop realitzat això hem d'executar l'script inclòs en la carpeta private per crear la base de dades i el contingut dels reptes.

En aquest script també conté un usuari amb perfil administratiu **admin (Usuari : admin / Password : admin)** d'accés al backend.

6.2 Sil·labari Kana

Figura 6.2 Sil.labari Kana

7 . Glossari

Terme	Definició
PHP	*PHP: Hypertext Preprocessor* Llenguatge de programació PHP es un llenguatge de programació a on el codi és executat en el servidor generant HTML i enviant-lo al client.
ASCII	*American Standard Code for Information Interchange* – Codi de caràcters basat en l'alfabet llatí .
DES	*Data Encryption Standard*- Algoritme de xifratge de bloc .
ECB	*Electronic code bloc.* Mode d'operació de DES.
CBC	*Cipher-block chaining*.Mode d'operació de DES.
CFB	*Cipher feedback* .Mode d'operació de DES.
OFB	*Output feedback*. Mode d'operació de DES.
RSA	*Rivest Shamir y Adleman* .Criptosistema de clau pública.
Kana	Terme genèric que es refereix als sil·labaris japonesos.
CAPTCHA	*Completely Automated Public Turing test to tell Computers and Humans Apart*
Apache	Servidor web HTTP de codi obert que implementa el protocol HTTP 1.1 /1.1
HTTP	*Hypertext Transfer Protoco*l és el protocol utilitzat en cada transacció de la world wide web.
SQL	*Structured Query Language . Llenguatge declaratiu d'accés a les bases de dades relacionals.*
IDE	*Integrated development environment* - Programari que s'utilitza per el desenvolupament del software
SSH2	*Secure Shell*. Protocol criptogràfic de xarxa utilitzat per comunicacions de dades segures a través de la xarxa.
X.509	És un estàndard UIT-T per a infraestructures de clau pública.
Rijndael	El criptosistema de Rijndael xifra blocs de text en clar de 128, 192 o 256 bits de longitud .
Twofish	Criptosistema simètric amb xifratge per blocs.
Blowfish	Criptosistema simètric amb xifratge per blocs.
RC4	Sistema de xifratge de flux . És un dels mes utiltzats.
RC2	Criptosistema de clau simètrica.

XAMPP	X= Qualsevol sistema operatiu Apache MySQL PHP Perl.

Taula 5

8 . Bibliografia

Materials de la UOC de les assignatures :

Criptografia

Altres materials :

Introduction to Criptography → https://class.coursera.org/crypto-preview - Curs de coursera impartit per Dan Boneh,

Pàgines web :

[1] *Twig - Documentation 2010-2012 Sensio Labs* Disponible a: http://twig.sensiolabs.org/doc/intro.html

[2] *Php manual* Disponible a: http://www.php.net/manual/en/

[3] *Algoritme RSA* Disponible a: http://190.90.112.209/http/criptografia/algoritmo_rsa.html

[4] *RSA crytoanalisis* Disponible a: http://www.cs.virginia.edu/~cmt5n/Classwork/Crypt/Mike/rsacrypt.html

[5] *RSA Encryption, Decryption, Prime calculator* Autor: Willem Van Iseghem Disponbile a :http://rsatools.wforums.net/

[6] *phpseclib: An Introduction phpseclib is licensed with the* MIT-license. Disponible a: http://phpseclib.sourceforge.net

[7] *Cipher Machines* Disponible a: http://ciphermachines.com/index

[8] *Navy N3/M4 Enigma Machine Emulator* . Autor Louise Dade. Disponible a: http://enigma.louisedade.co.uk/enigma.html

[9] *Crytool-online* © 1998 - 2014 CrypTool Project / Contributors Disponible a: http://www.cryptool-online.org

[10] *Cipher Machines and Cryptology* Autor : *Dirk Rijmenants ON3DZ 2004 - 2014* Disponible a: http://users.telenet.be/d.rijmenants/index.htm

[11] Google reCaptcha Disponible a: https://www.google.com/recaptcha/intro/index.html

[12] *Poedit Gettext Translations* Editor Disponible a: www.poedit.net

[13] T*wig y PHP para desarrollo web multilenguaje* . Autor: Luis.F. Cazares . Disponible a: http://cazaresluis.com/twig-y-php/

Blogs :

[1] *Informació relativa a wargames i diferents links* Disponible a: http://www.aegis.pe/2013/12/wargames-hacking-challenges.html

Llibres :

[1] *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C* (cloth) (Publisher: John Wiley & Sons, Inc.) Autor : Bruce Schneier ISBN: 0471128457 Publication Date: 01/01/96

[2] *Codebreakers. The story of secret writing.* Autor : David Kahn