Roberto Falconi, Salvatore Licitra
Progetto per il Laboratorio di Architetture Software e Sicurezza Informatica
Documentazione completa

Link a repository GitHub:
https://github.com/RobertoFalconi95/Kalypso

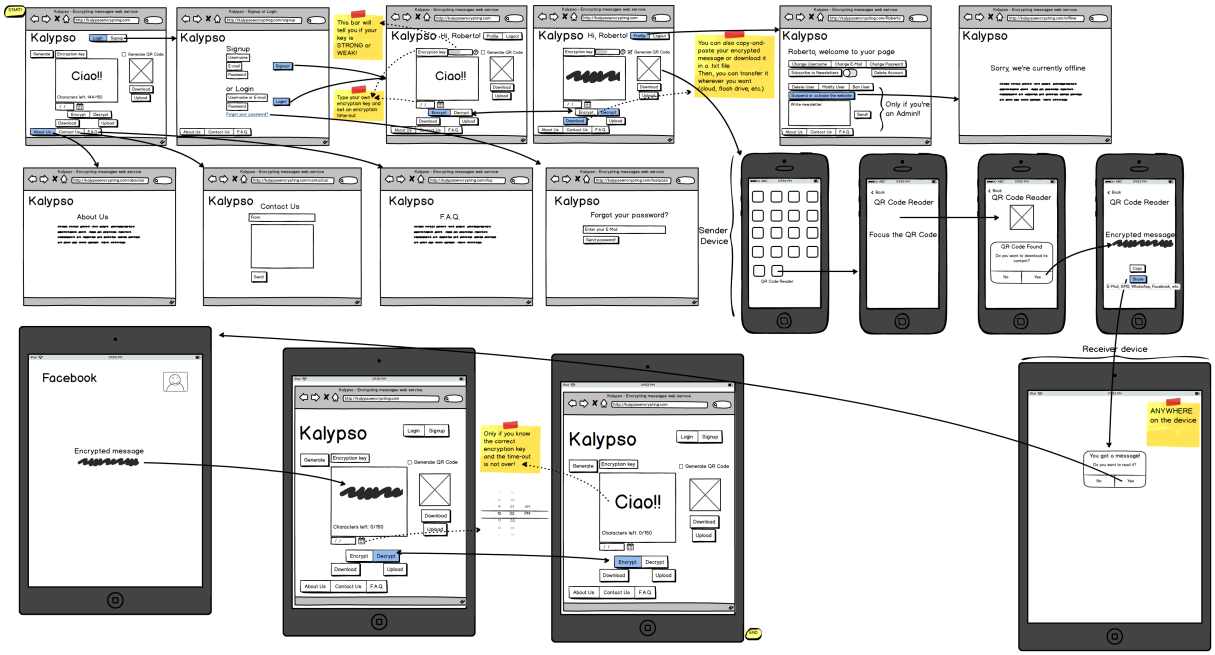
Link a Google Spreadsheets con tracking degli sprint:
https://docs.google.com/spreadsheets/d/1C6RYKo2PK_IFUdkNDsKCFGc_K27sW4KpYxzh5mLYOJI/edit?usp=sharing

User Stories

1. As an unregistered user, I want to sign up with username, e-mail and password so that I can become a user
2. As an unregistered user, I want to login with username or e-mail so that I can become a user
3. As a user, I want to have a personal profile so that I can logout from my session
4. As a user, I want to have settings so that I can restore my password if I lost it
5. As a user, I want to have a personal profile so that I can change my username
6. As a user, I want to have a personal profile so that I can change my e-mail
7. As a user, I want to have a personal profile so that I can change my password
8. As a user, I want to have a personal profile so that I can delete my account
9. As a user, I want to have a personal profile so that I can see my username in homepage
10. As a user, I want to have a personal profile so that I can subscribe to mailing list
11. As a user, I want to use the cryptography algorithm so that I can type an encryption key
12. As an unregistered user, I want to use the cryptography algorithm so that I can use an auto-generated encryption key
13. As a user, I want to use the cryptography algorithm so that I can get tips about choosing a good encryption key
14. As a user, I want to use the cryptography algorithm so that I can see the weakness of my personal encryption key
15. As a user, I want to use the cryptography algorithm so that I can encrypt unlimited characters
16. As an unregistered user, I want to use the cryptography algorithm so that I can see how many characters left to be encrypted
17. As an unregistered user, I want to use the cryptography algorithm so that I can set a time-out to a message to be decrypted
18. As an unregistered user, I want to use the cryptography algorithm so that I can download the encrypted message in a text file
19. As an unregistered user, I want to use the cryptography algorithm so that I can upload the encrypted message from a text file
20. As an unregistered user, I want to use the cryptography algorithm so that I can encrypt a message

21. As an unregistered user, I want to use the cryptography algorithm so that I can decrypt a message
22. As an unregistered user, I want to use QR Code so that I can transfer my encrypted message on my phone
23. As an unregistered user, I want to use the cryptography algorithm so that I can generate a QR Code with the encrypted message
24. As an unregistered user, I want to use the cryptography algorithm so that I can download the generated QR Code
25. As an unregistered user, I want to use the cryptography algorithm so that I can upload the generated QR Code
26. As an unregistered user, I want to see the F.A.Q. so that I can read it
27. As an unregistered user, I want to see a section About Us so that I can read it
28. As an unregistered user, I want to be able to contact developers thank to a Contact Us section so that I can get assistance or give feedback
29. As an unregistered user, I want to get a warning if the website is under maintenance so that I can know the status of the app
30. As a admin, I want to have special settings so that I can delete users
31. As a admin, I want to have special settings so that I can modify users account
32. As a admin, I want to have special settings so that I can ban users
33. As a admin, I want to have special settings so that I can suspend the website
34. As a admin, I want to have special settings so that I can activate the website
35. As a admin, I want to have a special setting so that I can send newsletters

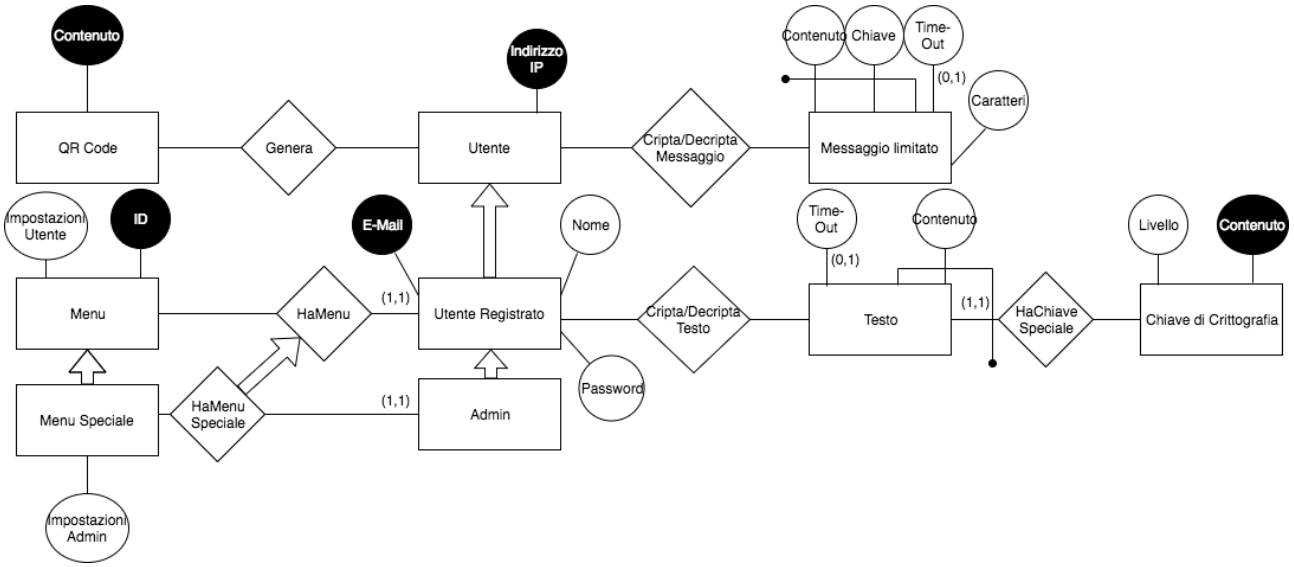
Mockups



Modello ER: requisiti

Di ogni utente interessa l'indirizzo IP (identificatore).
Alcuni utenti sono registrati, e di questi interessa nome, e-mail (identificatore) e password.
Gli utenti registrati possono accedere ad un menu, di cui interessano le impostazioni utente e l'ID (identificatore).
Alcuni utenti registrati sono admin, ed hanno accesso ad un particolare menu di amministrazione, di cui interessano le impostazioni di amministrazione.
Un utente può criptare o decriptare dei messaggi limitati, di cui interessa il contenuto, il numero di caratteri, un eventuale time-out e la chiave di crittografia (unica nell'ambito del contenuto).
Un utente registrato può criptare o decriptare dei testi di cui interessa il contenuto, un eventuale time-out e la chiave di crittografia (unica nell'ambito del contenuto); di quest'ultima interessa il contenuto (identificatore) e il livello di sicurezza.
Ogni utente può generare QR Code di cui interessa il contenuto (identificatore).

Modello ER: diagramma E-R



Dizionario dei dati: entità

Entità	Descrizione	Attributi	Identificatori
Homepage	Pagina principale	ID, About Us, Contact Us, F.A.Q.	ID
QR Code		Contenuto	Contenuto
Utente	Visitatore anonimo della pagina	Indirizzo IP	Indirizzo IP
Messaggio Limitato	Breve messaggio di testo da criptare o criptato	Contenuto, Caratteri, Time-Out, Chiave	Contenuto, Chiave
Menu	Pagina personale di un utente registrato	ID, Impostazioni utente	ID
Utente Registrato	Utente che ha deciso di iscriversi	Nome, E-Mail, Password	Indirizzo IP, E-Mail

Testo	Messaggio di testo lungo a piacere da criptare o criptato	Contenuto, Time-Out	Contenuto, Chiave di Crittografia
Chiave di crittografia	Chiave che permette la criptazione e la decriptazione	Contenuto, Livello di sicurezza	Contenuto
Menu Speciale	Pagina privata con impostazioni speciali	Impostazioni admin	ID
Admin	Speciale utente registrato che ha pieni poteri sulla web app	Indirizzo IP, Nome, E-Mail, Password	Indirizzo IP, E-Mail

Dizionario dei dati: relazioni

Relazione	**Descrizione**	**Componenti**	**Attributi**	**Identificatori**
Visita	La visita della Web App da parte di un utente	Homepage, Utente		
Genera	QR Code generato da un Utente	QR Code, Utente		
Cripta/Decripta Messaggio	Possibilità di criptare o decriptare un messaggio	Utente, Messaggio limitato		
Cripta/Decripta Testo	Possibilità di criptare o decriptare un testo	Utente Registrato, Testo		
HaChiaveSpeciale	Chiave di crittografia che può essere scelta a piacere	Testo, Chiave di Crittografia		
HaMenu	Appartenenza ad un utente di un menù con le impostazioni	Menu, Utente Registrato		
HaMenuSpeciale	Appartenenza ad un admin di un menù riservato	Menu Speciale, Admin		

Dizionario dei dati: attributi

Attributi	Entità/Relazione	Dominio	Descrizione
ID	Homepage	Intero	Identificatore
F.A.Q.	Homepage	Stringa	UX
Contact Us	Homepage	Stringa	UX
About Us	Homepage	Stringa	UX
Indirizzo IP	Utente	Intero	Provenienza
Contenuto	QR Code	Stringa	Messaggio
Contenuto	Messaggio limitato	Intero	Messaggio
Caratteri	Messaggio limitato	Intero	Limite massimo
Time-Out	Messaggio limitato	Data	Limite massimo
Chiave	Messaggio limitato	Stringa	Chiave crittografica
ID	Menu	Intero	ID
Impostazioni Utente	Menu	Stringa	UX
Nome	Utente registrato	Stringa	UX
E-Mail	Utente registrato	Stringa	UX
Password	Utente registrato	Stringa	UX
Contenuto	Testo	Intero	Messaggio
Time-Out	Testo	Data	Limite massimo
Contenuto	Chiave di crittografia	Stringa	Identificatore
Livello	Chiave di crittografia	Stringa	UX
Impostazioni Admin	Menu speciale	Stringa	UX

Dizionario dei dati: vincoli di cardinalità

Sull'attributo Time-Out dell'entità Messaggio limitato e dell'entità Testo è stato utilizzato un vincolo di cardinalità "(0,1)" in quanto opzionale.

Un utente registrato e un admin hanno accesso, rispettivamente, a uno e un solo menu privato, per tanto è stato utilizzato un vincolo di cardinalità "(1,1)".

Ad un messaggio limitato (o ad un testo), è associata una ed una sola chiave di crittografia e quindi il vincolo utilizzato è stato "(1,1)".

Dizionario dei dati: vincoli esterni

Al fine di evitare perdita di leggibilità è consigliabile evitare l'utilizzo di vincoli esterni.

A tal proposito al momento della progettazione concettuale sono stati abilmente evitati.

Struttura controllo degli accessi: ruoli e diritti di accesso alle funzionalità disponibili
Un visitatore può accedere alle pagine Home, F.A.Q., Contact Us, About Us e Newsletter.
Può criptare messaggi di lunghezza limitata e non può scegliere una chiave di crittografia a piacere; può tuttavia impostare un time-out sui messaggi ed ha pieno accesso alle funzionalità di download e upload del messaggio in formato .txt e alle funzionalità legate al QR Code.

Un utente registrato ha gli stessi diritti di un visitatore ma può criptare un messaggio di qualsiasi lunghezza, utilizzare la chiave di crittografia che desidera ed accedere alle impostazioni per modificare il proprio account.

Un admin ha accesso alle funzionalità di un utente e può modificare non solo il suo account, ma anche quello di qualsiasi altro utente, che può anche cancellare o bannare.

Piano dei test