Improving the Security Using 2Flip in VANET

J.Lavanya
Department of Information Technology, II-MTech, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur.

Dr.S.Sivananaitha Perumal
Department of Information Technology, HOD, Dr.Sivanthi Aditanar College of Engineering, Tiruchendur.

Abstract – Here a Two-Factor Lightweight Privacy-preserving authentication scheme (2FLIP) has been used to enhance the security of VANET communication. 2FLIP employs the decentralized certificate authority (CA) and the password-based two-factor authentication (2FA) to achieve the goals. Based on the decentralized CA, 2FLIP only requires several extremely lightweight hashing processes and a fast message-authentication-code operation for message signing and verification between vehicles. The proposed scheme provides strong privacy preservation that the adversaries can never succeed in tracing any vehicles, even with all RSUs compromised.Moreover, it achieves strong nonrepudiation , even if he is not the only driver of the vehicle. Extensive simulations reveal that 2FLIP is feasible and has an outstanding performance of nearly 0-ms network delay and 0% packet-loss ratio.

Index Terms – Privacy, strong nonrepudiation, two-factor authentication, vehicular ad-hoc network (VANET).

1. INTRODUCTION

In a VANET, every vehicle is equipped with an onboard unit (OBU), through which it could communicate wirelessly with other vehicles and road side units (RSUs) over one or more hops. Thus, a large-scale wireless network could be constructed, which utilizes dedicated short-range communications (DSRC) [1] to realize high-speed reliable data exchange of vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R), simultaneously achieving features of mobile ad hoc and communicatively opportunistic. The fabulous characteristics of the VANET are significant to traffic management and roadside safety. In addition, V2V aims at transmitting basic safety information between vehicles to facilitate warnings to drivers concerning impending crashes [2]. Security requirements of a VANET could be divided into two types: a basic type due to the inheritance from a mobile ad-hoc network (MANET) and a special type concerning vehicular communications. Traditional security threats in wireless communication, such as eavesdropping, forgery, and modification,could be easily taken advantage of in VANETs. This incurs the basic security goals, such as resilience to forgery or modification of messages and nonrepudiation. Particularly for vehicular communication, the VANET system must collect and transmit only anonymous" data from mobile users for mandatory applications and keep such data "anonymous" until securely destroyed.

Among previous studies [3], [4] one of the most public recognized idea to ensure the security of VANETs and privacy of vehicles is privacy-preserving authentication (PPA). Until now, there already suggest a large quantity of PPA schemes for VANETs, some of which are based on public key infrastructure (PKI) and are employing traditional digital signature techniques to authenticate messages. Such schemes have some downsides: 1) vulnerable availability due to effortless denial-of-service (DoS) attack and 2) collapse of scheme caused by high packet-loss ratio. In this paper, proposed a Two-Factor LIghtweight Privacy- preserving (2FLIP) authentication scheme for VANETs, which introduces the idea of a two-factor authentication technique to VANETs mainly by utilizing message-authentication-code (MAC) and hash operations for improving the security and privacy of VANETs. 2FLIP only requires several extremely lightweight one-way hash operations and a MAC generation operation, for message signing, and a hash function along with one fast MAC regeneration, for verification.

A digital signature verification process is only launched when a vehicle needs system key updating, which would not affect the performance. As far as we are concerned, 2FLIP is the first authentication scheme that achieves both strong privacy preservation and DoS resilience for secure VANET communication without employing a symmetric or asymmetric key mechanism; additionally, it is also the first authentication scheme trying to authenticate multiple users of one single vehicle, which conditionally traces each one of them in postevent investigation.

The advantages of our proposed 2FLIP scheme are as follows.

1) Strong privacy preservation

2FLIP is able to guarantee level 3 privacy: authentication, anonymity, and unlinkability. Moreover, responsibilities of RSUs are purposefully weakened, which leads to strong privacy, such that, even if all RSUs are compromised, malevolent parties still could not pry into the real identities of vehicles.

2) Strong nonrepudiation

2FLIP provides the basic nonrepudiation that the vehicle could not deny the message from itself. Moreover,considering multiple drivers of one vehicle could also not deny himself from sending the message. A driver has to first hold the telematics device and then offers his password (transformed from some biometrics, e.g.,a fingerprint, or an iris scan) to start the vehicle. The evidences generated from the password are transmitted to a CA after some proper time interval, which are used to trace each driver conditionally, hence providing strong nonrepudiation.

3) Secure system key update

Once the system key is leaked, 2FLIP provides a mechanism to restore the whole system by updating the system key at a low cost, which is essential for a practical system.

4) Secure offline password update

Biological password embedded in a telematics device could be updated without connection to RSUs or CA, therefore providing support to flexible use right transfer.

5) Extremely lightweight and efficient

2FLIP employs only hash operations coupled with MAC generation to accomplish the signing of messages and a fast MAC regeneration for verification, subsequently achieving a significant reduction of nearly 102–103 times in computational consumption compared with subsisting schemes. This makes 2FLIP DoS-resilient compared with concurrent schemes, even in large-scale VANET with large vehicle density.

6) Low certificate management overhead, communication cost, and network delay

In 2FLIP, a dynamic pseudoidentity and a short MAC are carried within a message packet, rather than digital signature and certificate. On one hand, all certificate revocation list (CRL)-related overhead is eliminated whether it is responsible for by CA or vehicles. On the other hand, in the comparison with other current schemes, our proposed 2FLIP achieves a decrease of 55.24%–77.52% in communication costs and a considerably lower network delay.

2. RELATED WORK

Numerous schemes have been proposed to improve the security and conditional privacy preservation in VANETs. They could be classified into three categories: 1) schemes based on pseudonymous certificate; 2) schemes based on group signature; 3) hybrid schemes that combine the pseudonymous authentication and group signature.

1) *Pseudonymous-certificate-based schemes*

Pseudonymous-authentication-based schemes first link many pairs of private key and pseudonymous certificate to a pseudoidentity. Afterward, a source vehicle could utilize its private key to sign messages, and all receivers could authenticate the messages by the corresponding pseudonymous certificate.

2) *Group-signature-based schemes*

The cord idea of group-based schemes is that group members are hidden in a group, with real identity covered and privacy protected. They suggested a privacy-preserving authentication scheme based on group signature and identity (ID)-based signature [7] (GSIS).

3)Hybrid schemes

Hybrid schemes combine pseudonymous authentication protocol, digital signature, MAC, and other authentication technologies to make a tradeoff between computation efficiency, CRL size, bandwidth consumption, verification delay, and so on.

3. PROPOSED TWO-FACTOR LIGHTWEIGHT PRIVACY SCHEME

2FLIP employs mainly two core methods to achieve the design goals presented in the previous chapter: CA decentralization and the biological-password-based 2FA.(Fig.1)

A. System Initialization and Entity Registration

As for vehicle and driver registration, we have the following.

1)For Vehicle i , along with its biological driver, first it submits its real identity ID_i , $\gamma_{i,u} = h(pw_{i,u})$, and $Info_i$ (e.g.,engine serial number, date of manufacture, and vehicle owner) to the CA through secure channels (e.g.,drive to CA to submit information personally).

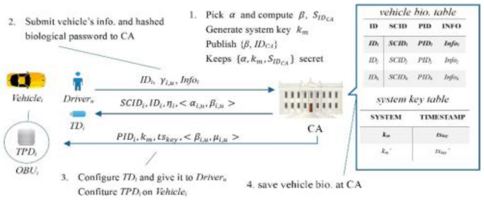

2. Submit vehicle's info. and hashed biological password to CA
1. Pick α and compute β, $S_{ID_{CA}}$
Generate system key k_m
Publish $\{\beta, ID_{CA}\}$
Keeps $\{\alpha, k_m, S_{ID_{CA}}\}$ secret
vehicle bio. table
ID SCID PID INFO
ID_i $SCID_i$ PID_i $Info_i$
ID_j $SCID_j$ PID_j $Info_j$
ID_k $SCID_k$ PID_k $Info_k$
system key table
SYSTEM TIMESTAMP
k_m ts_{key}
k_m' ts_{key}'
Vehicle$_i$
Driver$_u$
$ID_i, \gamma_{i,u}, Info_i$
$SCID_i, ID_i, \eta_i, < \alpha_{i,u}, \beta_{i,u} >$
TD_i
CA
$PID_i, k_m, ts_{key}, < \beta_{i,u}, \mu_{i,u} >$
TPD_i
OBU_i
3. Configure TD_i and give it to Driver$_u$
Confiture TPD_i on Vehicle$_i$
4. save vehicle bio. at CA

Fig. 1. Initialization phase of 2FLIP

2) CA checks the correctness of these information (usually with assistance of the national vehicle management department). If the information is valid, CA randomly picks $PID_i \in Z^*_q$ as initial pseudoidentity of Vehicle i , and $SCID_i$ for TD_i .

3) CA computes the following to acquire the biological password verifier and the biological password keeper: $\eta_i = h(ID_i || SCID_i || PID_i) \oplus h(SCID_i || k_m)$ $\mu_i = h(ID_i || \gamma_{i,u} || PID_i) \oplus h(SCID_i || k_m)$ $\alpha_{i,u} = h(\gamma_{i,u} \oplus PID_i)$, $\beta_{i,u} = PID_i \oplus h(SCID_i \oplus \gamma_{i,u})$. Here, $\alpha_{i,u}$, $\beta_{i,u}$ is employed as a biological verifier to authenticate driver's identity and $\beta_{i,u}$ is used to protect the $\beta_{i,u}$, $\mu_{i,u}$ and update the biological password locally.

4) Finally, CA saves ID i , SCID i , PID i , Info i of Vehicle i to a user & bio table and writes {SCID i , ID i , η i , α i,u ,β i,u } to a telematics device TD i , which shall be distributed to the corresponding biological driver, and preloads {PID i , k m , ts key , β i,u , μ i,u } on TPD i .

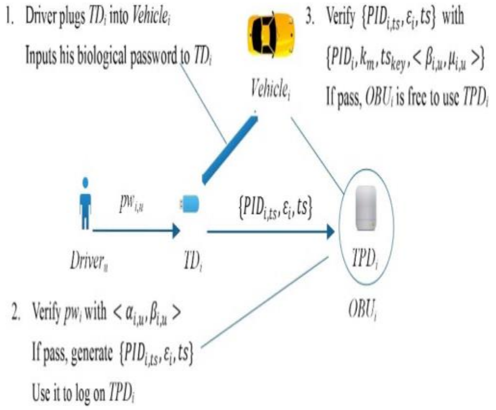

1. Driver plugs TD_i into $Vehicle_i$
Inputs his biological password to TD_i
3. Verify $\{PID_{i,ts}, \varepsilon_i, ts\}$ with
$\{PID_i, k_m, ts_{key}, < \beta_{i,u}, \mu_{i,u} >\}$
If pass, OBU_i is free to use TPD_i
$Vehicle_i$
$pw_{i,u}$
$\{PID_{i,ts}, \varepsilon_i, ts\}$
$Driver_u$
TD_i
TPD_i
OBU_i
2. Verify pw_i with $< \alpha_{i,u}, \beta_{i,u} >$
If pass, generate $\{PID_{i,ts}, \varepsilon_i, ts\}$
Use it to log on TPD_i

Fig. 2. Driver identity verification and TPD login of 2FLIP.

B. Driver Identity Verification and TPD Login

Before a driver joins the VANET, he needs to first pass the driver identity verification. After that, whenever the vehicle generates a new message and broadcasts it, the TPD login process should be launched instantly.

C. Message Signing

When the vehicle generates a new message payload m, TD i redoes the TPD login phase to facilitate the TPD with up-to-date dynamic pseudoidentity PID i,ts . If the TPD login is finished, TPD i would calculate the message authentication value of the m like σ i = mac k m (PID i,ts ||h(m||k m)||ts) and broadcasts {PID i,ts , σ i ts, m} to nearby vehicles.

D. Message Verification

TPD j calculates σ i ∗ = mac k m (PID i,ts ||h(m||k m)||ts) to verify the legitimacy of the message after Vehicle j receives a packet {PID i,ts , σ i , ts, m} from Vehicle i . If σ i ∗ ! = σ i returns false, Vehicle j then accepts the message and employs the message for application use; otherwise, it rejects the message.

E. System Key Update

System key k m is the cornerstone of the whole system and is protected by the TPD; thus, an adversary cannot take advantage of the TPD even if the vehicle is stolen. In order to further enhance the system security, we introduce a system key updating strategy to update k m periodically. Update of the system key ought to be carried out by the national vehicle management department on vehicle annual inspection and implemented by CA and distributed RSUs.

F. Vehicle Revocation

Once Vehicle i is judged as invalid, CA would perform the revocation process of it to notify all other vehicles. It is direct and quick. CA broadcasts {PID i , sg rev } to all vehicles, in which sg rev is the signature of PID i calculated by sg rev = Sign S ID (PID i). When Vehicle i receives the revocation message, it would verify the source legitimacy of it. If legitimate, TPD i deletes all the secret materials preloaded in the registration phase, including {PID i , k m , ts key , β i,u , μ i,u }; thus,TPD i is made illegal and is no longer able to generate legitimate messages.

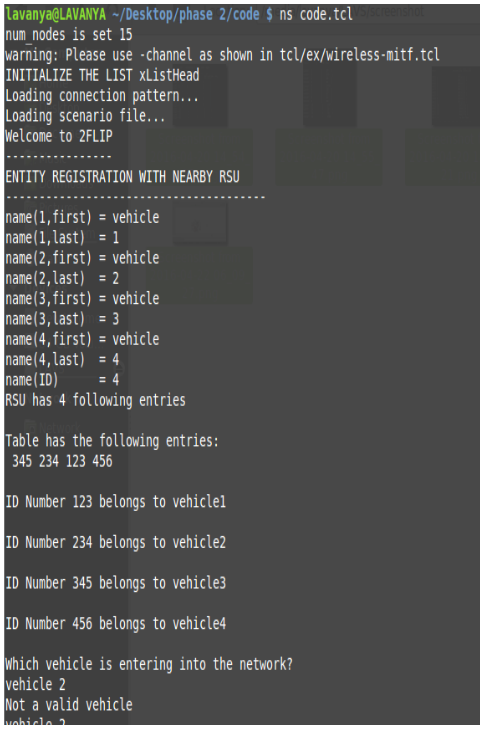
G. Message Tracing

Although the anonymity and unlinkability are preserved, CA is able to trace the source vehicle and biological driver of each disputable message in after-event investigation

H. Biological password update

In the proposed scheme, benign flexibility is provided that such biological password update could be implemented offline without any contact with CA or RSUs but only relying on the telematics device and TPD.

4. PERFORMANCE EVALUATION



```
lavanya@LAVANYA ~/Desktop/phase 2/code $ ns code.tcl
num_nodes is set 15
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Welcome to 2FLIP
---------------
ENTITY REGISTRATION WITH NEARBY RSU
---------------------------------------
name(1,first) = vehicle
name(1,last)  = 1
name(2,first) = vehicle
name(2,last)  = 2
name(3,first) = vehicle
name(3,last)  = 3
name(4,first) = vehicle
name(4,last)  = 4
name(ID)      = 4
RSU has 4 following entries

Table has the following entries:
 345 234 123 456

ID Number 123 belongs to vehicle1

ID Number 234 belongs to vehicle2

ID Number 345 belongs to vehicle3

ID Number 456 belongs to vehicle4

Which vehicle is entering into the network?
vehicle 2
Not a valid vehicle
vehicle 2
```

Fig:3 System initialization

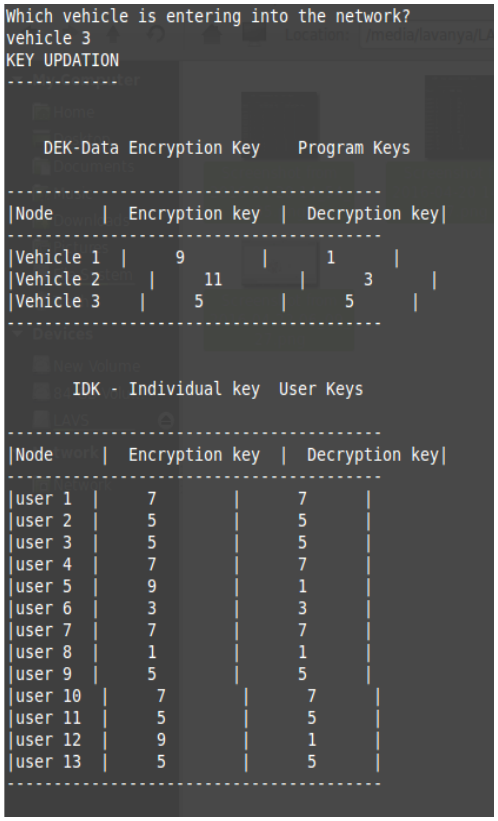
The properties of 0 message loss ratio and about 100% signatures verified facilitate 2FLIP with resilience to DoS attack both in computation and in communication, which significantly increases the availability and stability of the VANET. Considering the aforementioned analysis of simulations,[5] 2FLIP turns out to have the lowest average message delay, the lowest message loss ratio, and the highest of signature verified percentage. Although VAST also performs well, it should be noted that it can never provide essential security features, such as unlinkability, conditional traceability, nonrepudiation, and others.[6]

System Initialisation and Entity registration

ID of the vehicle is generated by the nearby RSU. Upon receiving the ID of the vehicle, it decides to enter into the network or not. If the vehicle is valid, then next steps are proceeded.(Fig 3).

Key updation

Keys are generated by the server for each user. Hence Key generation, Key distribution,Encryption and Decryption (Fig 4).

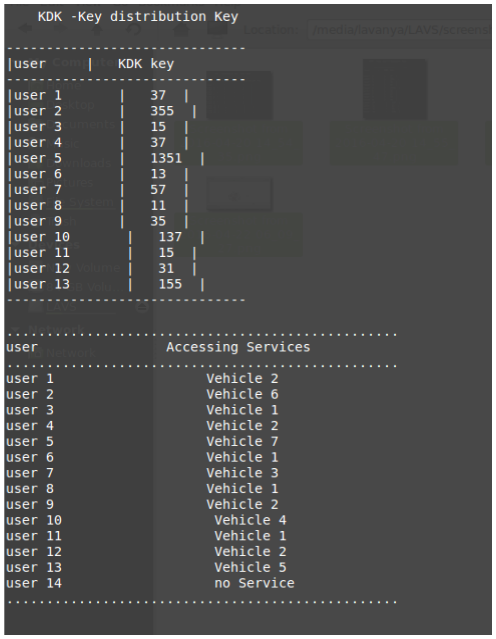


```
Which vehicle is entering into the network?
vehicle 3
KEY UPDATION
-----------

    DEK-Data Encryption Key    Program Keys

----------------------------------------
|Node      |  Encryption key  |  Decryption key|
----------------------------------------
|Vehicle 1  |     9        |     1      |
|Vehicle 2    |     11        |      3      |
|Vehicle 3    |     5        |      5      |
----------------------------------------

       IDK - Individual key  User Keys

----------------------------------------
|Node      |  Encryption key  |  Decryption key|
----------------------------------------
|user 1  |     7        |      7      |
|user 2  |     5        |      5      |
|user 3  |     5        |      5      |
|user 4  |     7        |      7      |
|user 5  |     9        |      1      |
|user 6  |     3        |      3      |
|user 7  |     7        |      7      |
|user 8  |     1        |      1      |
|user 9  |     5        |      5      |
|user 10  |     7        |      7      |
|user 11  |     5        |      5      |
|user 12  |     9        |      1      |
|user 13  |     5        |      5      |
----------------------------------------
```

Fig:4 Key updation

Message broadcasting

Data is send from server and it is encrypted by the public key and send it to the Vehicle and the message will be decrypted by the private key. Then individual user keys will be provided to the user(Fig 5).

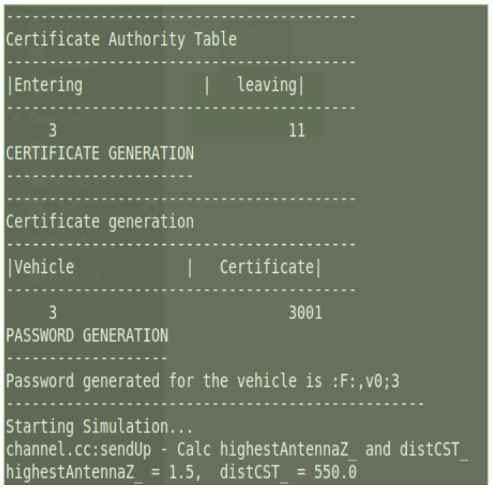


```
    KDK -Key distribution Key

------------------------------
|user     |    KDK key
------------------------------
|user 1        |    37  |
|user 2        |    355  |
|user 3        |    15  |
|user 4        |    37  |
|user 5        |    1351  |
|user 6        |    13  |
|user 7        |    57  |
|user 8        |    11  |
|user 9        |    35  |
|user 10        |    137  |
|user 11        |    15  |
|user 12        |    31  |
|user 13        |    155  |
------------------------------

................................................
user                    Accessing Services
................................................
user 1                       Vehicle 2
user 2                       Vehicle 6
user 3                       Vehicle 1
user 4                       Vehicle 2
user 5                       Vehicle 7
user 6                       Vehicle 1
user 7                       Vehicle 3
user 8                       Vehicle 1
user 9                       Vehicle 2
user 10                       Vehicle 4
user 11                       Vehicle 1
user 12                       Vehicle 2
user 13                       Vehicle 5
user 14                       no Service
................................................
```

Fig: 5 Message broadcasting

Certificate & Password generation

Certificate will be generated for each vehicle which is entering into the network and password will be given so that non-repudiation is achieved (Fig 6).



```
----------------------------------------
Certificate Authority Table
----------------------------------------
|Entering              |  leaving|
----------------------------------------
    3                          11
CERTIFICATE GENERATION
--------------------
----------------------------------------
Certificate generation
----------------------------------------
|Vehicle             |   Certificate|
----------------------------------------
    3                          3001
PASSWORD GENERATION
------------------
Password generated for the vehicle is :F:,v0;3
-----------------------------------------------
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
```

Fig:6 Certificate & Password generation

5. CONCLUSION

The proposed a 2FLIP preserving authentication scheme, which employs two core methods: decentralization of CA and password-based 2FA. Based on the decentralization of CA, the proposed scheme requires only several extremely lightweight hashing processes, and a fast MAC generation is needed for message signing and a hash function along with one fast MAC regeneration for verification, which increases efficiency of computation and communication. Extensive simulations reveal that the novel scheme is feasible and has an outstanding performance on message signing/verification, message loss ratio, and network delay. Moreover, decentralization of CA makes the certificate transmitting not necessary, which removes the overhead of certificate management. Through biological-password-based 2FA, 2FLIP achieves strong nonrepudiation that any biological anonym driver could be conditionally traced. To the best of our knowledge, 2FLIP is the first authentication scheme that achieves both strong privacy preservation and DoS resilience for secure VANET communication with the benefits of combining the two core methods.

REFERENCES

[1] L. Armstrong, “Dedicated Short Range Communications (DSRC) Home,” 2002.

[2] J. Harding et al., “Vehicle-to-vehicle communications: Readiness of V2V technology for application,” Nat. Highway Traffic Safety Admin.,Washington, DC, USA, Tech. Rep. DOT-HS-812-014, Aug. 2014.

[3] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[4] L. Zhang, Q. Wu, A. Solanas, and D.-F. Josep, “A scalable robust authentication protocol for secure vehicular communications,” IEEE Trans. Veh.Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

[5] A. Keränen, J. Ott, and T. Kärkkäinen, “The ONE simulator for DTN protocol evaluation,” in *Proc. 2nd Int. Conf. Simul. Tools Techn.*, 2009,pp. 55.

[6] F. Wang, “twoflip_proverif, ProVerif program for phases in 2FLIP scheme,” 2015, [Online]. Available: https://github.com/finleywang/twoflip_proverif

[7] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Proc. Adv. Cryptology-Crypto*, ser. LNCS, vol. 196, 1984, pp. 47–53,New York, Springer-Verlag.

[8] http://kylewbanks.com/blog/Simple-XOR-Encryption-Decryption-in-Cpp

[9] http://codereview.stackexchange.com/questions/77519/simple-password-encryption-decryption-in-c

[10] http://www.cplusplus.com/forum/general/73404/

[11] https://www.cs.utexas.edu/~mitra/honors/soln.html