LABORATORY

CEL62: Cryptography and System Security
Winter 2021

Experiment 7:	**Creating and Reading QR Codes** **Ref:** **https://www.linux-magazine.com/Online/Features/Generating-QR-Codes-in-Linux**

Note: Students are advised to read through this lab sheet before doing experiment. On-the-spot evaluation may be carried out during or at the end of the experiment. Your performance, teamwork/Personal effort, and learning attitude will count towards the marks.

Sumeet Haldipur
2019130018
TE Comps

Experiment 6: Creating and Reading QR codes

1 OBJECTIVE

Creating and Reading QR Codes for given exercise

2 INTRODUCTION

With the right tools, you can create your own QR code squares with information you want to share on a business card, in a letter, or on your website.

Read errors of unreliable, one-dimensional bar codes often caused interruptions in industrial production, prompting companies like Toyota and its subsidiary Denso Wave to develop as early as 1994 a new code for acquiring stock data. The new matrix bar code was designed to store more information than the traditional bar code and to stay legible, even if the label was dirty, wrinkled, or partially destroyed.

The quick response code, or QR code, comprises a matrix of square dots instead of the usual lines. Measuring up to 177 by 177 dots, the QR code encodes up to 4,296 characters, compared with a bar code that encodes just 13.

Thanks to numerous free reader apps for smartphones, QR codes have gained in popularity in recent years. Posters, catalogs, magazines, business cards, and even television screens display the small squares, offering additional information or URLs for microsites.

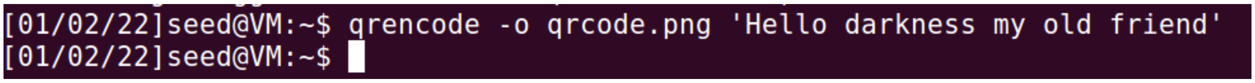
Data Grabber

If you want to encode your address into a QR code for a business card, you could try one of the many services on the Internet. However, restrictions typically apply. For example, some services allow only QR codes in a certain size or in limited quantities. Also, you never know for sure, what the services do with your data. For example, some sites explicitly allow sharing and selling the data to third parties in their terms of use, more or less pre-programming an increase in junk mail in the future. Fortunately, several QR code tools can help you avoid these problems in Linux.

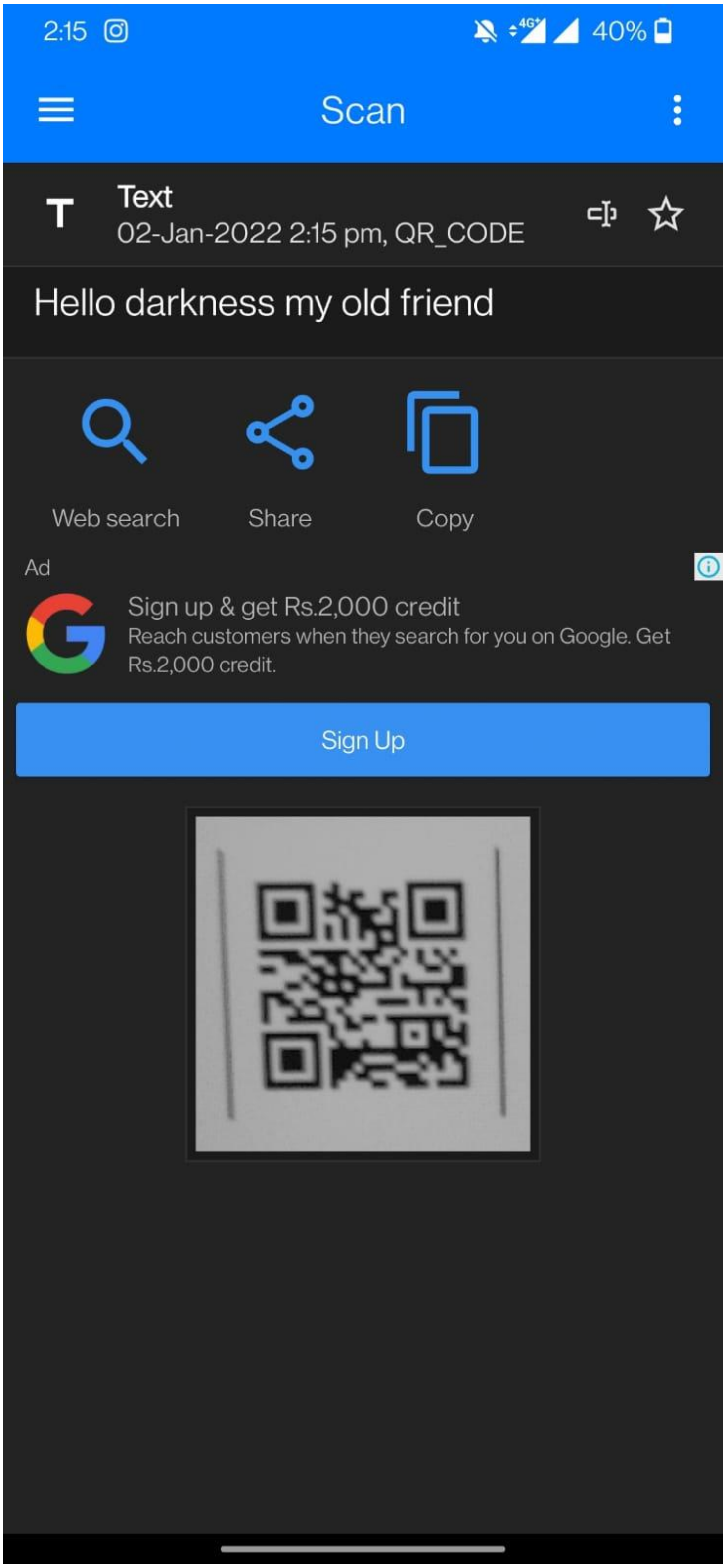
3 PROCEDURE/TASK

The quickest way to create a QR code is with the Qrencode command-line utility. Any major distribution can install Qrencode via the package manager. The following command then creates a QR code containing the text “Hello World!”:

$ qrencode -o qrcode.png 'Hello World!'



```
[01/02/22]seed@VM:~$ qrencode -o qrcode.png 'Hello darkness my old friend'
[01/02/22]seed@VM:~$ 
```



T

Text

02-Jan-2022 2:15 pm, QR_CODE

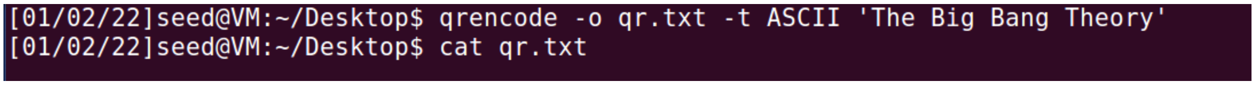
Hello darkness my old friend

QR Code relevant Hello darkness my old friend will pop up: Qrencode encoding the string "Hello darkness my old friend" as a QR code and storing it in the qrencode.png file.

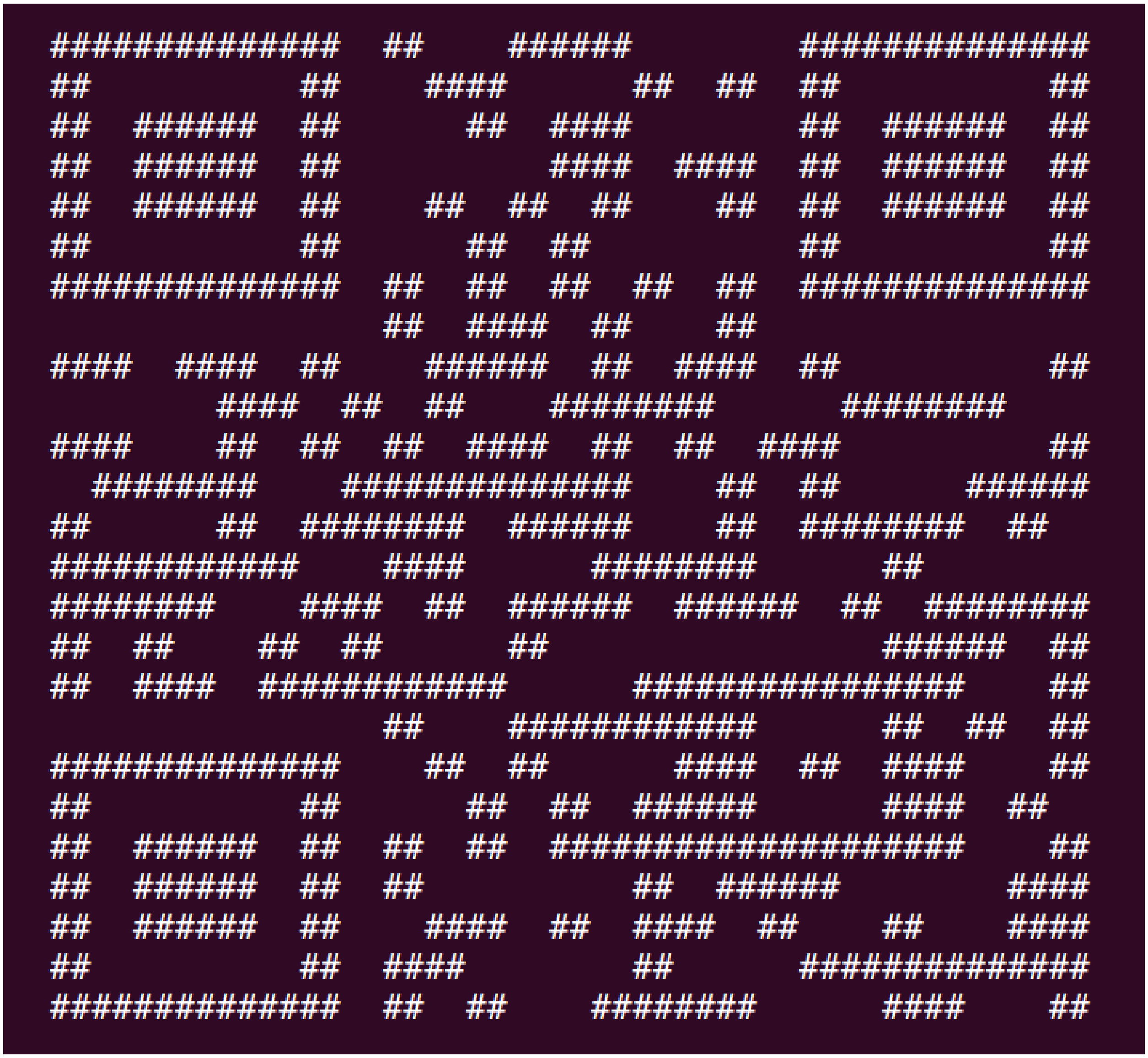
The generated QR code ends up in the *qr.png* file. If the file already exists, it's overwritten without prompting. If you have at least version 3.3.0 (*qrencode -V*), Qrencode can generate an EPS graphic,

$ qrencode -t EPS -o qrcode.eps 'Hello World!'

or ASCII output.



```
[01/02/22]seed@VM:~/Desktop$ qrencode -o qr.txt -t ASCII 'The Big Bang Theory'
[01/02/22]seed@VM:~/Desktop$ cat qr.txt
```

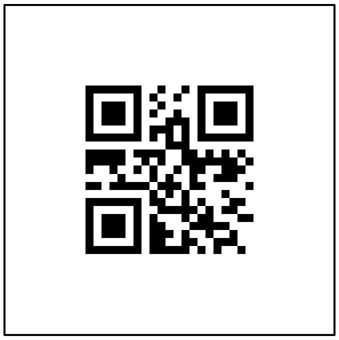


```
##############  ##    ######        ##############
##          ##    ####      ##  ##  ##          ##
##  ######  ##      ##  ####        ##  ######  ##
##  ######  ##          ####  ####  ##  ######  ##
##  ######  ##    ##  ##  ##    ##  ##  ######  ##
##          ##      ##  ##          ##          ##
##############  ##  ##  ##  ##  ##  ##############
                ##  ####  ##    ##
####  ####  ##    ######  ##  ####  ##          ##
        ####  ##  ##    ########      ########
####    ##  ##  ##  ####  ##  ##  ####          ##
  ########    ##############    ##  ##      ######
##      ##  ########  ######    ##  ########  ##
############    ####      ########      ##
########    ####  ##  ######  ######  ##  ########
##  ##    ##  ##      ##                ######  ##
##  ####  ############      ################    ##
                ##    ############      ##  ##  ##
##############    ##  ##      ####  ##  ####    ##
##          ##      ##  ##  ######      ####  ##
##  ######  ##  ##  ##  ####################    ##
##  ######  ##  ##          ##  ######        ####
##  ######  ##    ####  ##  ####  ##    ##    ####
##          ##  ####        ##      ##############
##############  ##  ##    ########      ####    ##
```

Outputting QR codes in ASCII characters just for fun. Each # corresponds to a dot.

In the QR code image, the software creates a white border the width of one dot. This facilitates the process of deciphering the code for programs or the smartphone later on. If desirable, you can increase or decrease the edge with the *-m* parameter; in the following example the border width would be 10 code pixels:

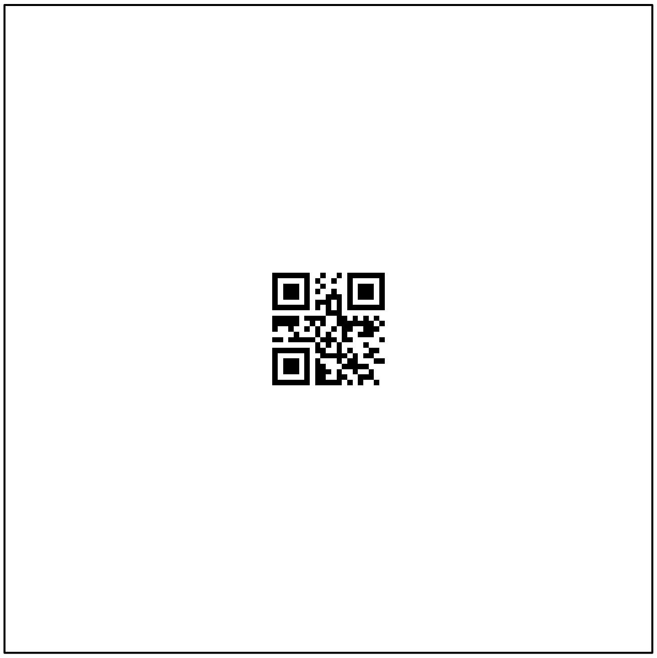
```
$ qrencode -m 10 -o qrcode.png 'Hello World!'
```



If you are saving the QR code in PNG format, the *-s* parameter specifies the height of a black QR code pixel. By default, Qrencode draws every black dot three by three pixels. The program creates a slightly smaller QR code with quite a wide margin with the following command:

```
$ qrencode -s 2 -m 10 -o qrcode.png 'Hello World!'
```

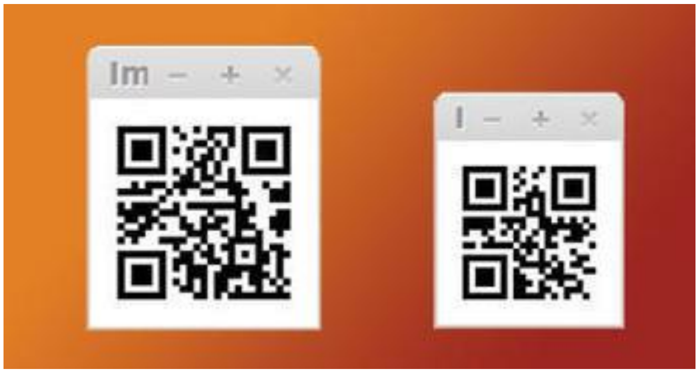
A white border appears around the QR code that is exactly 20 screen pixels wide (10 QR code dots in width, with each dot two pixels). If you are creating EPS images, the only parameter available is *-m*; *-s* moves the entire QR code out of the image in this case. To control the resolution of PNGs further, use the *-d* parameter to define the dpi.



Tolerance

Besides the specified data, the QR code contains additional error correction information. If a portion of the image is damaged, it allows you to reconstruct the missing or illegible data. The more additional information the QR code contains, the more heavily damaged it can be without becoming useless.

Increasing the error tolerance increases the size of the image because you need more black dots



Both QR codes contain the text Hello World!; the one on the left uses the highest error correction level, H, and therefore is more robust – but also larger.

The QR code standard thus uses four levels of error correction: *H* level allows you to read all data if 30 percent of the QR code is destroyed, *Q* level if 25 percent is unreadable, and *M* level if just 15 percent is unintelligible. At the lowest level, *L*, only 7 percent of the data can be faulty. In Qrencode, the *-l* parameter selects the error correction level. The possible values are pretty much what you would expect: *L*, *M*, *Q*, and *H*.

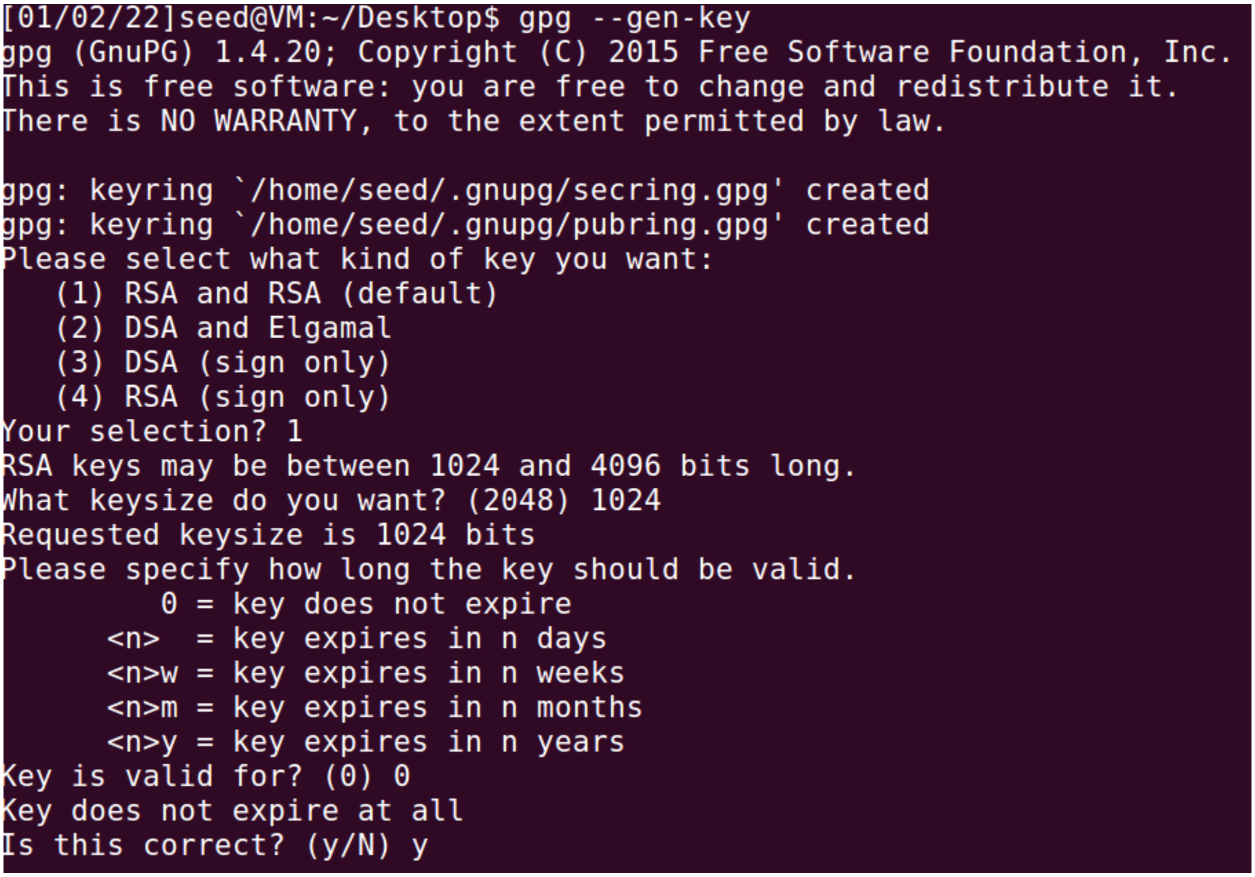
Of the tested programs, Portable QR-Code Generator offers the greatest functionality. Data entry is also convenient in a variety of tabs. Qrencode creates QR codes more quickly, and it is easy to scripted so you generate QR codes in batches. KBarcode4-light is deprecated, but it is the only program that can generate PDF files; the EPS images created by Qrencode offer similar output.

EXERCISE

TPO of SPIT has asked you to submit simple QR code of your CV so that company can make off line process to create short list of potential candidates. Hence as a part of exercise create CV showing your Profile, Ability and Capability and generate QR code of CV. This QR code can only be shared between you and company. You will provide your digital signature as an authentication to company. Once authentication is successful company is able to scan this QR code of your CV.

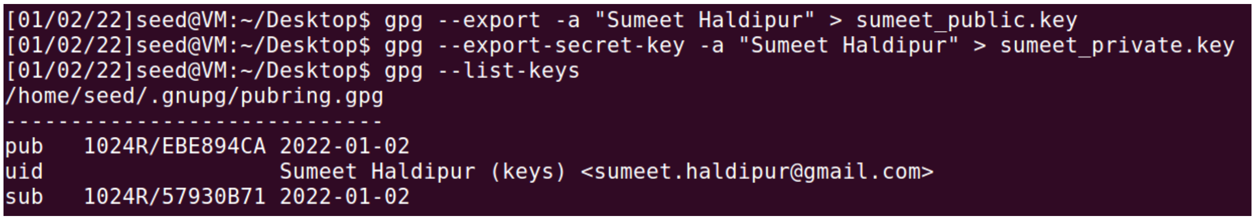
Show Implementation steps that you will generate QR code and sign it with your digital signature. Share it with your colleague from same lab with who is capable to verify your digital signature. Successful verification makes scanning of QR code feasible. Show you creativity in terms of robustness of generating digital signature, generating of QR code and Scanning of QR code if relevant secret key is entered.

Creating new keys for encryption



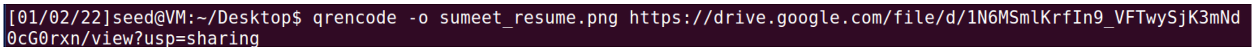
```
[01/02/22]seed@VM:~/Desktop$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: keyring `/home/seed/.gnupg/secring.gpg' created
gpg: keyring `/home/seed/.gnupg/pubring.gpg' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y
```

Exporting newly generated public and private keys.

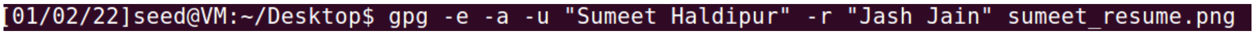


```
[01/02/22]seed@VM:~/Desktop$ gpg --export -a "Sumeet Haldipur" > sumeet_public.key
[01/02/22]seed@VM:~/Desktop$ gpg --export-secret-key -a "Sumeet Haldipur" > sumeet_private.key
[01/02/22]seed@VM:~/Desktop$ gpg --list-keys
/home/seed/.gnupg/pubring.gpg
-----------------------------
pub   1024R/EBE894CA 2022-01-02
uid                  Sumeet Haldipur (keys) <sumeet.haldipur@gmail.com>
sub   1024R/57930B71 2022-01-02
```

Encoding the URL of the Resume using qrencode



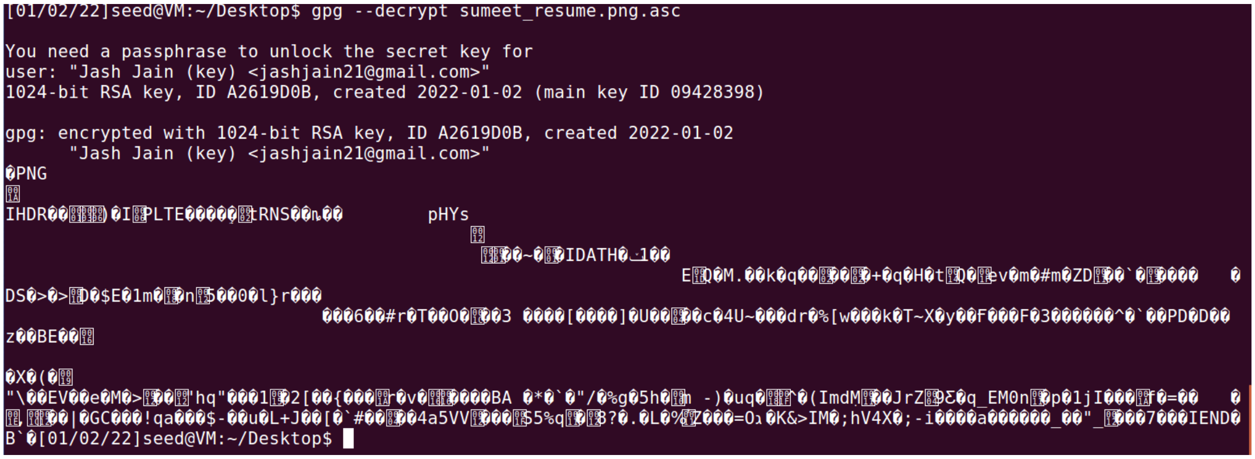
```
[01/02/22]seed@VM:~/Desktop$ qrencode -o sumeet_resume.png https://drive.google.com/file/d/1N6MSmlKrfIn9_VFTwySjK3mNd
0cG0rxn/view?usp=sharing
```



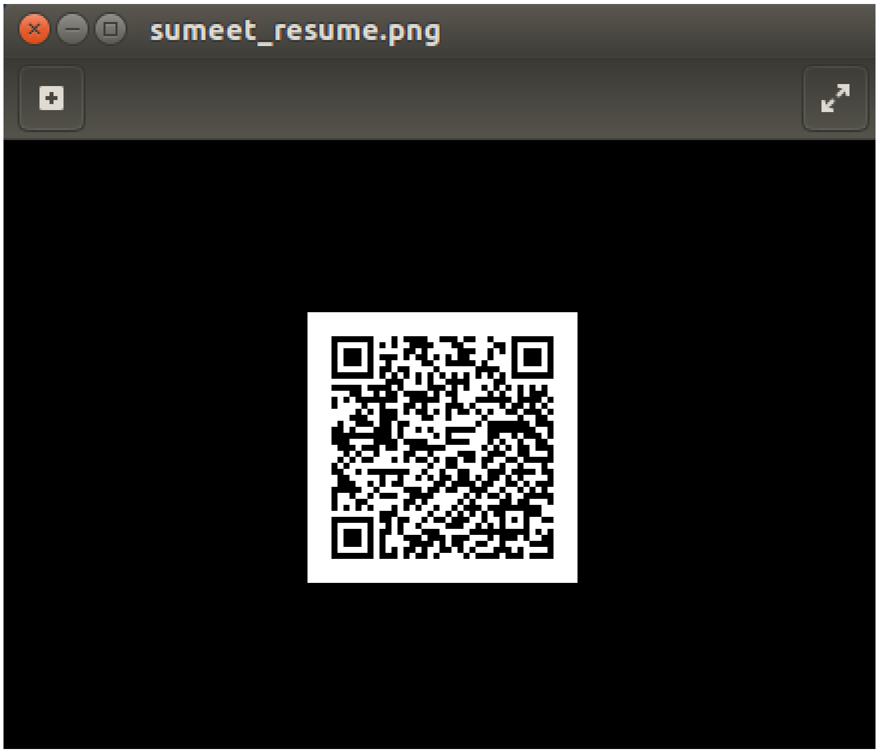
```
[01/02/22]seed@VM:~/Desktop$ gpg -e -a -u "Sumeet Haldipur" -r "Jash Jain" sumeet_resume.png
```

Once encrypted using the keys of Sumeet Haldipur, user Jash Jain is able to

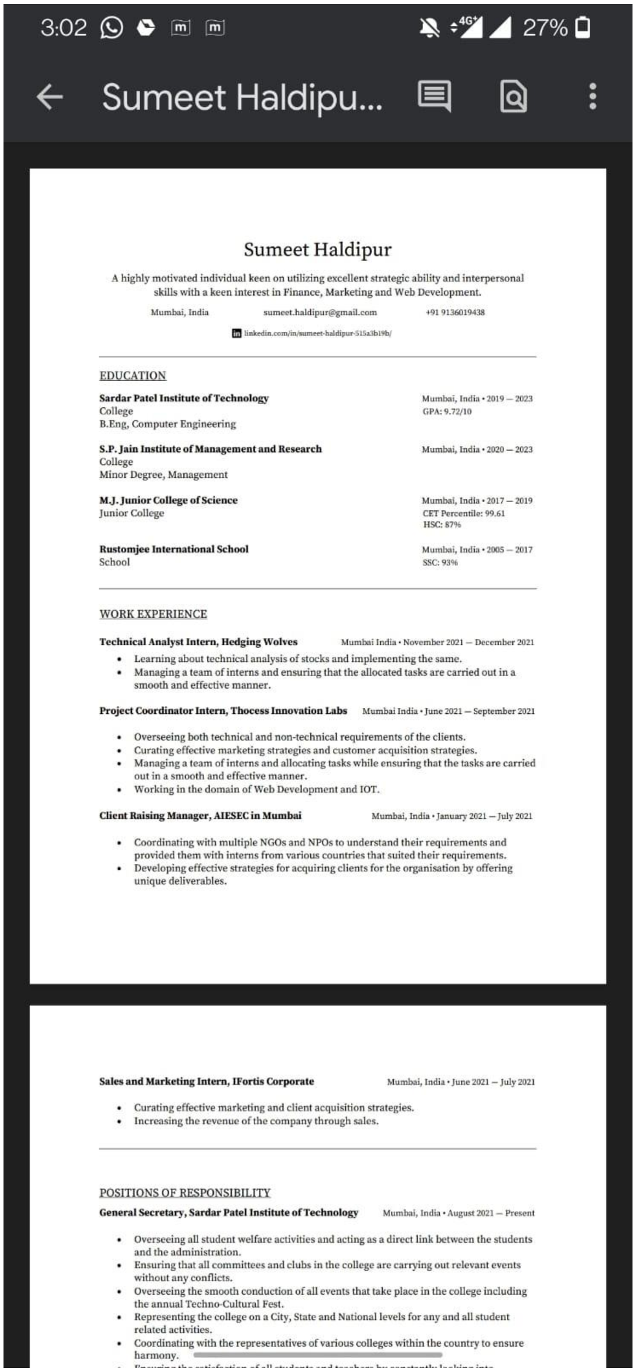
decrypt the same using his own keys.
This makes sure that only the intended users are able to access the resume from the QR Code.



```
[01/02/22]seed@VM:~/Desktop$ gpg --decrypt sumeet_resume.png.asc

You need a passphrase to unlock the secret key for
user: "Jash Jain (key) <jashjain21@gmail.com>"
1024-bit RSA key, ID A2619D0B, created 2022-01-02 (main key ID 09428398)

gpg: encrypted with 1024-bit RSA key, ID A2619D0B, created 2022-01-02
      "Jash Jain (key) <jashjain21@gmail.com>"
�PNG
�
IHDR�����)�I�PLTE�������tRNS��ɲ��        pHYs
                                                   �
                                                    ���~��IDATH�ـ1��
                                                                           E��M.��k�q�����+�q�H�t��Q��ev�m�#m�ZD���`�����   �
DS�>�>�D�$E�1m���n�5���0�l}r���
                              ���6��#r�T��O���3 ����[����]�U����c�4U~���dr�%[w���k�T~X�y��F���F�3������^�`��PD�D��
z��BE���

�X�(��
"\��EV��e�M�>�����'hq"���1��2[��{�����r�v������BA �*�`�"/�%g�5h���n -)�uq����`�(ImdM����JrZ�Ꮽ�q_EM0n��p�1jI�����f�=��   �
�,����|�GC���!qa���$-��u�L+J��[�`#�����4a5VV������5%q����3?�.�L�%��Z���=Oɿ�K&>IM�;hV4X�;-i����a������_��"_����7���IEND�
B`�[01/02/22]seed@VM:~/Desktop$ 
```



Checking the output of scanning the QR code on an external device (Mobile Phone)



Sumeet Haldipur

A highly motivated individual keen on utilizing excellent strategic ability and interpersonal skills with a keen interest in Finance, Marketing and Web Development.

Mumbai, India   sumeet.haldipur@gmail.com   +91 9136019438

linkedin.com/in/sumeet-haldipur-515a3b19b/

EDUCATION

Sardar Patel Institute of Technology   Mumbai, India • 2019 — 2023
College   GPA: 9.72/10
B.Eng, Computer Engineering

S.P. Jain Institute of Management and Research   Mumbai, India • 2020 — 2023
College
Minor Degree, Management

M.J. Junior College of Science   Mumbai, India • 2017 — 2019
Junior College   CET Percentile: 99.61
HSC: 87%

Rustomjee International School   Mumbai, India • 2005 — 2017
School   SSC: 93%

WORK EXPERIENCE

Technical Analyst Intern, Hedging Wolves   Mumbai India • November 2021 — December 2021

- Learning about technical analysis of stocks and implementing the same.
- Managing a team of interns and ensuring that the allocated tasks are carried out in a smooth and effective manner.

Project Coordinator Intern, Thocess Innovation Labs   Mumbai India • June 2021 — September 2021

- Overseeing both technical and non-technical requirements of the clients.
- Curating effective marketing strategies and customer acquisition strategies.
- Managing a team of interns and allocating tasks while ensuring that the tasks are carried out in a smooth and effective manner.
- Working in the domain of Web Development and IOT.

Client Raising Manager, AIESEC in Mumbai   Mumbai, India • January 2021 — July 2021

- Coordinating with multiple NGOs and NPOs to understand their requirements and provided them with interns from various countries that suited their requirements.
- Developing effective strategies for acquiring clients for the organisation by offering unique deliverables.

Sales and Marketing Intern, IFortis Corporate   Mumbai, India • June 2021 — July 2021

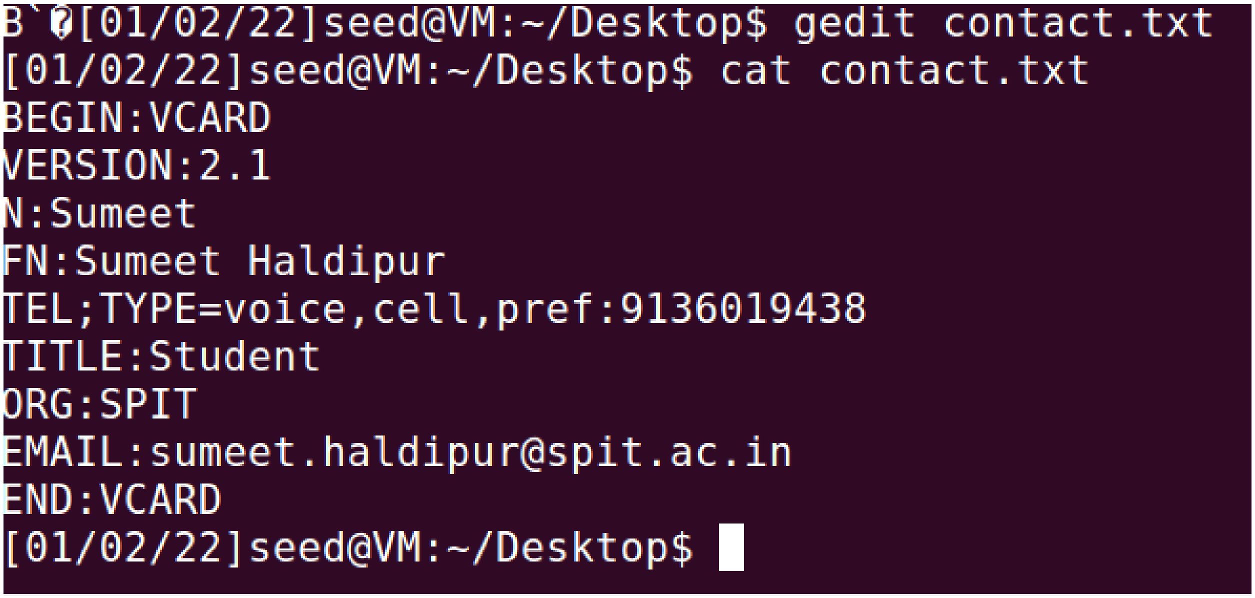
- Curating effective marketing and client acquisition strategies.
- Increasing the revenue of the company through sales.

POSITIONS OF RESPONSIBILITY

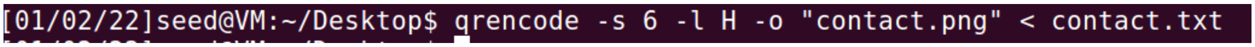
General Secretary, Sardar Patel Institute of Technology   Mumbai, India • August 2021 — Present

- Overseeing all student welfare activities and acting as a direct link between the students and the administration.
- Ensuring that all committees and clubs in the college are carrying out relevant events without any conflicts.
- Overseeing the smooth conduction of all events that take place in the college including the annual Techno-Cultural Fest.
- Representing the college on a City, State and National levels for any and all student related activities.
- Coordinating with the representatives of various colleges within the country to ensure harmony.
- Ensuring the satisfaction of all students and teachers by constantly looking into

Creating a custom contact card and encapsulating the information in a QR Code

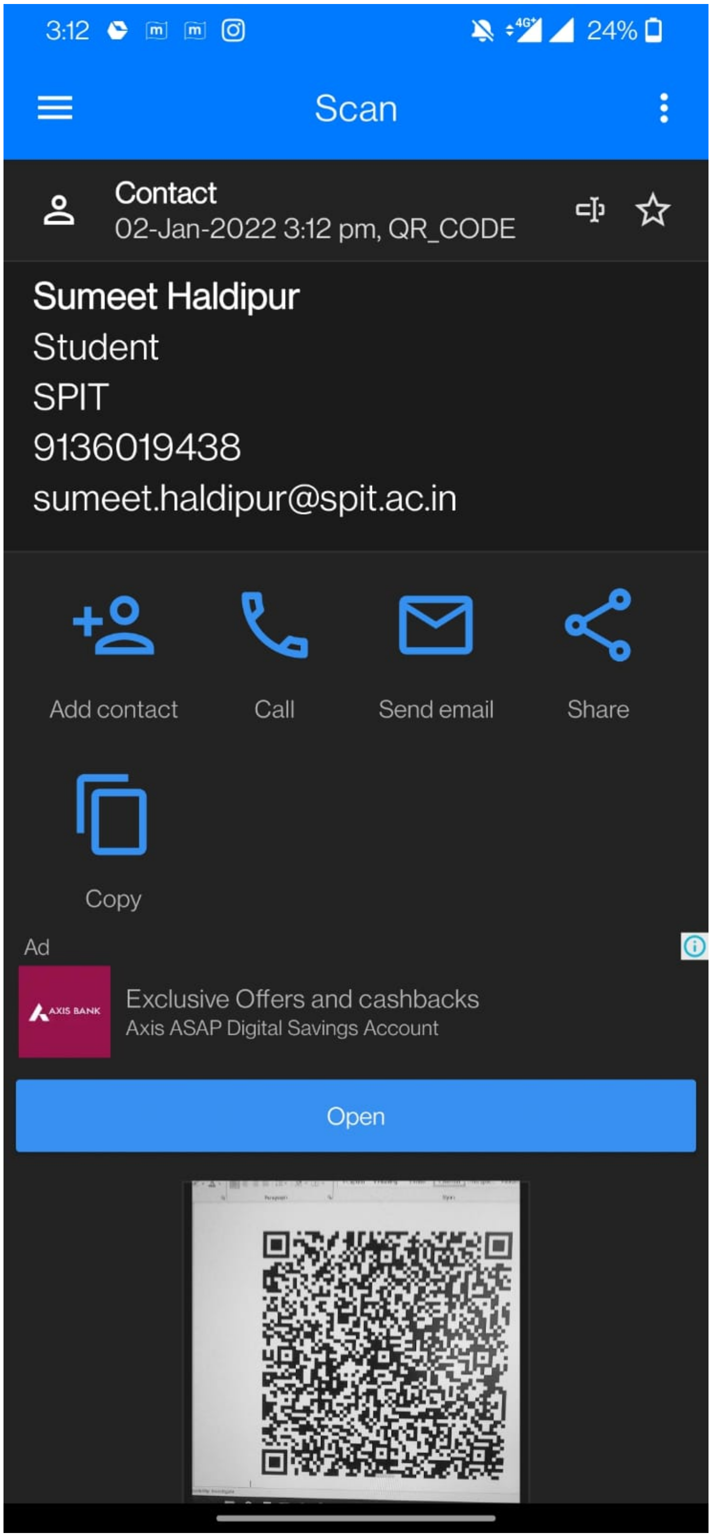


```
B`�[01/02/22]seed@VM:~/Desktop$ gedit contact.txt
[01/02/22]seed@VM:~/Desktop$ cat contact.txt
BEGIN:VCARD
VERSION:2.1
N:Sumeet
FN:Sumeet Haldipur
TEL;TYPE=voice,cell,pref:9136019438
TITLE:Student
ORG:SPIT
EMAIL:sumeet.haldipur@spit.ac.in
END:VCARD
[01/02/22]seed@VM:~/Desktop$ 
```



```
[01/02/22]seed@VM:~/Desktop$ qrencode -s 6 -l H -o "contact.png" < contact.txt
```

Checking the output of scanning the contact QR code on a mobile device.



Contact
02-Jan-2022 3:12 pm, QR_CODE

Sumeet Haldipur
Student
SPIT
9136019438
sumeet.haldipur@spit.ac.in

CONCLUSION:

1. QR codes are an easy and quick way to transmit information,
2. The security levels of QR codes can be set depending on how confidential/secure we want the information contained in it to be.
3. QR codes also provide error correction measures so that information can be extracted from the code even if part of the code is corrupted.
4. QR code themselves can be encrypted, so that only people with keys to the encrypted message can scan the code.

GitHub link: https://github.com/sumeethaldipur/CSS_LAB