

Homework Assignment 1

Ans 1).

Two experiments through which we can glean the PPI (Protected Personal Information) of the faculty and staff of IIIT Delhi.

- There are many sites which are government warehouses, have lots of governmental data shared by people and are available online. This can be of great importance to us for securing PPI(Protected Personal Information) of faculty and staff of IIIT-Delhi.
MTNL Directory(<http://phonebook.bol.net.in/>),
Voter List(<http://ceodelhi.gov.in/OnlineErms/ElectorSearch.aspx>),
PAN Card(<https://tin.tin.nsdl.com/tan/servlet/PanStatusTrack>),
Driving Licence Detail(<https://dlpay.dimts.in/dldetail/>), etc serve as of great importance to find PPI. So PPI such as home address, driving licence, telephone number, of faculty can be taken from these sites.
- The faculty and staff have their resume uploaded online. So, this can be of quite importance to us. This has lot of information like when the person completed his matriculation, higher secondary, Bachelor or Master's. With social networking sites such as Facebook and Twitter we can merge the above collected information and extract PPI of the staff at IIITD. We can calculate Date Of Birth or age, and find telephone Number, father's name, etc. Moreover we can also get login name or handle through social networking sites like Facebook.

Ans 2).

To measure the 'strength' of passwords:

- We can set a threshold that password length should be greater than or equal to this length.
- We can see if it contains capital letters, special characters, and not a dictionary word.
- We can develop password meters which determine the strength of the given password by using above parameters to measure the strength
- We should measure randomness or entropy by checking that same characters or consecutive characters should not be used. There should be

proper care taken so that characters are as random as possible which makes extremely difficult or virtually impossible to predict the password.

- We can also use one time passwords, that is it produces a unique key as a function of time to login. This increases the security.
- We can also use challenge-response system for authentication.

Good practices to choose a password:

- 1). Never pick names of special places, family person, sports person, etc. as passwords.
- 2). Dictionary words should be avoided as they can be easily found by brute force checking whether it matches with any word.
- 3). Password should be of at least 8 bits with digits, alphabets and special characters.
- 4). We should take care that the strong password could be memorised as well. For that we can use different techniques (like fitting in a sentence).
- 5). Pass phrases are good only if it is memorisable. They are difficult to predict.

We can encourage people to adopt these measures. We can tell them how easy it is to guess passwords if one's password has low randomness and could be easily predicted. Small passwords can be easily found using brute force.

People should be informed about what are the consequences if their passwords are leaked (and how it would affect their privacy).

We should tell them that they can use passphrases which could be memorised or use pronounceable paraphrase instead as they can be easily learnt and are quite safe. We can show people examples like: Have long Password of Length8 is better in comparison to pas13#sa\$%ss.

So, proper justifications will enable people to understand the importance of strong password and proper techniques would allow them to form one.

Ans 3).

I have taken privacy policy of Flipkart(<http://www.flipkart.com/s/privacypolicy>) and would quote various points of OECD and FTC Principles into it.

I have quoted the parts specifying OECD and FTC principles.

Purpose Specification Principle: The purpose for which data should be collected should be specified at the time of data collection.

“We use personal information to provide the services you request. To the extent we use your personal information to market to you, we will provide you the ability to opt-out of such uses. We use your personal information to resolve

disputes; troubleshoot problems; help promote a safe service; collect money; measure consumer interest in our products and services, inform you about online and offline offers, products, services, and updates; customize your experience; detect and protect us against error, fraud and other criminal activity; enforce our terms and conditions; and as otherwise described to you at the time of collection.”

Security Safeguards Principle: Personal data should be protected and loss, unauthorised access, modification or disclosure of data should be taken care of.

“Our Website has stringent security measures in place to protect the loss, misuse, and alteration of the information under our control. Whenever you change or access your account information, we offer the use of a secure server. Once your information is in our possession we adhere to strict security guidelines, protecting it against unauthorized access.”

Collection Limitation Principle

There should be limitation on personal data collected and should be collected only if the user is ready to give it.

“We collect personally identifiable information (email address, name, phone number, credit card / debit card / other payment instrument details, etc.) from you when you set up a free account with us. While you can browse some sections of our Website without being a registered member, certain activities (such as placing an order) do require registration. We do use your contact information to send you offers based on your previous orders and your interests.”

So, I will compare privacy policies of Flipkart, Amazon, and Paytm.

Differences:

1). Use Limitation Principle:

Flipkart:

"We may share personal information with our other corporate entities and affiliates. These entities and affiliates may market to you as a result of such sharing unless you explicitly opt-out."

Amazon:

"Information about our customers is an important part of our business and we are not in the business of selling it to others. Amazon.in shares customer information only as described below and with Amazon.com, Inc. and the

subsidiaries which Amazon.com, Inc., controls and that are either subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice."

Paytm:

"We will not sell, share or rent your personal information to any 3rd party or use your email address/mobile number for unsolicited emails and/or SMS. Any emails and/or SMS sent by Paytm will only be in connection with the provision of agreed services & products and this Privacy Policy."

So we see that Flipkart and Amazon share the user's personal information with third parties but Paytm is very keen on security and does not reveal personal information of the user to the third parties.

2). Individual Participation:

Flipkart:

"We value the trust you place in us. That's why we insist upon the highest standards for secure transactions and customer information privacy."

Amazon:

"Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian."

Paytm:

"When you browse through Paytm, we may collect information regarding the domain and host from which you access the internet, the Internet Protocol [IP] address of the computer or Internet service provider [ISP] you are using, and anonymous site statistical data."

So we see that Flipkart and Paytm can be used by anyone but Amazon allows only.

Similarity:

1). Purpose Specification Principle

Flipkart:

"We use personal information to provide the services you request. To the extent we use your personal information to market to you, we will provide you the ability to opt-out of such uses. We use your personal information to resolve disputes; troubleshoot problems; help promote a safe service; collect money; measure consumer interest in our products and services, inform you about online and offline offers, products, services, and updates; customize your experience; detect and protect us against error, fraud and other criminal activity; enforce our terms and conditions; and as otherwise described to you at the time of collection."

Amazon.in:

"Snapdeal collects, uses, stores and processes Your Information for any purpose as may be permissible under applicable laws (including where the applicable law provides for such collection, usage, storage or processes in accordance with the consent of the user) connected with a function or activity of each of Snapdeal entities."

Paytm:

"We use personal information to provide you with services & products you explicitly requested for, to resolve disputes, troubleshoot concerns, help promote safe services, collect money, measure consumer interest in our services, inform you about offers, products, services, updates, customize your experience, detect & protect us against error, fraud and other criminal activity, enforce our terms and conditions, etc."

So we see each of the three have their purpose specified clearly for which they collect the personal information.

2). Collection Limitation

Flipkart:

"When you use our Website, we collect and store your personal information which is provided by you from time to time. Our primary goal in doing so is to provide you a safe, efficient, smooth and customized experience. This allows us to provide services and features that most likely meet your needs, and to customize our Website to make your experience safer and easier. More importantly, while doing so we collect personal information from you that we consider necessary for achieving this purpose."

Amazon:

“Information You Give Us: We receive and store any information you enter on our Web site or give us in any other way. Click here to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.”

Paytm:

“Personal Information means and includes all information that can be linked to a specific individual or to identify any individual, such as name, address, mailing address, telephone number, email ID, credit card number, cardholder name, card expiration date, information about your mobile phone, DTH service, data card, electricity connection, Smart Tags and any details that may have been voluntarily provide by the user in connection with availing any of the services on Paytm”

So, we see that all three have specified which personal data they collect and there is limit to which personal data is collected and is collected only on consent of the individual.

3). Security Safeguard Principle

Flipkart:

“Our Website has stringent security measures in place to protect the loss, misuse, and alteration of the information under our control. Whenever you change or access your account information, we offer the use of a secure server. Once your information is in our possession we adhere to strict security guidelines, protecting it against unauthorized access.”

Amazon:

“We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input in addition to maintaining security of your information as per the International Standard IS/ISO/IEC 27001 on "Information Technology Security Techniques Information Security Management System-Requirements".”

So we see that all the three have stringent security measures and personal data is protected against any loss, modification, etc.

Paytm:

“Paytm has stringent security measures in place to protect the loss, misuse, and alteration of the information under our control. Whenever you change or access

your account information, we offer the use of a secure server. Once your information is in our possession we adhere to strict security guidelines, protecting it against unauthorized access.”

Use this comparative study to come with a policy for my own organization:

- First of all I should specify clearly what personal data would I collect and how, that is Collection Limitation. If I develop e-commerce site, I will collect PII such as name, age, date of birth, IP, PAN card, etc.
- Secondly, there should be purpose specification for which data is collected. There should be proper justification for which personal data is collected. If I develop e-commerce site, I would specify that these things are collected for keeping track of a person and ensuring that product is being at correct place.
- There should also be security safeguards to ensure that there is no loss or modification of personal data of an individual. So, this will be of quite importance in my privacy policy.
- Personal data should not be disclosed, made available to any third party without consent of individual. So, there should be proper attention to use limitation too.

Ans 4).

Similarity:

The Vigenere cipher is a variation of the Caesar cipher. Both are substitution ciphers. Caesar cipher is a shift cipher in which we are given the number by which we have to shift all the characters.

For eg: shift A by 6 leads to G. The Vigenere cipher is also shift cipher and is like Caesar cipher but uses a phrase.

Difference:

In Caesar cipher, every character is shifted by same number of place. So, we can say it is mono-alphabetic. In Vigenere cipher, shift is by different places based on the specified keyword. So, it can be called as poly-alphabetic.

Vigenere cipher is more difficult to decode. It is because in Caesar cipher, one has to shift all characters by same number of bits. Encrypted text looks like plain text. However, in Vigenere cipher shift of each character depends on keyword chosen. So normal frequency methods cannot be used to decode it and hence it is safe.

Feistel Cipher: From a Feistel Cipher, many block ciphers are derived. Eg: DES

It is a symmetric cipher, that is it uses same method for encryption and decryption.

Fiestal scheme is like this:

Plain Text: (L0, R0)

For encryption:

for $i = 0, \dots, N$

$$L[i+1] = R[i]$$

$$R[i+1] = L[i] \text{ xor } F(R[i], \text{key}[i])$$

Ciphertext = (R[N+1], L[N+1])

For decryption:

for $i = N, \dots, 0$

$$L[i] = R[i+1] \text{ xor } F(L[i+1], \text{key}[i])$$

$$R[i+1] = L[i+1]$$

We can specify number of rounds in fiestal scheme. It depends on security and also usability.

/* Code:

#include <bits/stdc++.h>


```
using namespace std;
```

```
map< char, string > ma;
```

```
map< string, string > ma_rev;
```

```
string mess_bin;
```

```
void init()
```

```
{
```

```
    ma[ '0' ] = "0000";
```

```
    ma[ '1' ] = "0001";
```

```
    ma[ '2' ] = "0010";
```

```
    ma[ '3' ] = "0011";
```

```
    ma[ '4' ] = "0100";
```

```
    ma[ '5' ] = "0101";
```

```
    ma[ '6' ] = "0110";
```

```
    ma[ '7' ] = "0111";
```

```
    ma[ '8' ] = "1000";
```

```
    ma[ '9' ] = "1001";
```

```
    ma[ 'A' ] = "1010";
```

```
    ma[ 'B' ] = "1011";
```

```
    ma[ 'C' ] = "1100";
```

```
    ma[ 'D' ] = "1101";
```

```
    ma[ 'E' ] = "1110";
```

```
    ma[ 'F' ] = "1111";
```

```
    ma_rev[ "0000" ] = "0";
```

```
    ma_rev[ "0001" ] = "1";
```

```

    ma_rev[ "0010" ] = "2";
    ma_rev[ "0011" ] = "3";
    ma_rev[ "0100" ] = "4";
    ma_rev[ "0101" ] = "5";
    ma_rev[ "0110" ] = "6";
    ma_rev[ "0111" ] = "7";
    ma_rev[ "1000" ] = "8";
    ma_rev[ "1001" ] = "9";
    ma_rev[ "1010" ] = "A";
    ma_rev[ "1011" ] = "B";
    ma_rev[ "1100" ] = "C";
    ma_rev[ "1101" ] = "D";
    ma_rev[ "1110" ] = "E";
    ma_rev[ "1111" ] = "F";
}

```

```

string to_binary( string st )
{
    string anss = "";
    int i;
    for(int i=0; i<(int)st.length(); i++)
    {
        anss += ma[ st[i] ];
    }

    return anss;
}

```

```

string LSH( string st )
{
    char ch = st[27], ch2;
    for(int i=26; i>=0; i--)
    {
        ch2 = st[i];
        st[i] = ch;
        ch = ch2;
    }
    st[27] = ch;

    return st;
}

```

```

string f_function( string R_1, string keyy )
{
    string extraa = mess_bin.substr(0, 48), anss = "", compressed;

```

// Extending R0 to 48 bits so that RO and key is of same length according to following function.

```

int extend[48] = {
    1, 2, 3, 4, 5, 6, 7, 8,
    9, 10, 11, 12, 13, 14, 15, 16,
    17, 18, 19, 20, 21, 22, 23, 24,
    25, 26, 27, 28, 29, 30, 31, 32,
    1, 2, 3, 4, 5, 6, 7, 8,
    9, 10, 11, 12, 13, 14, 15, 16

```

```
};
```

```
for( int i=0; i<47; i++ )
```

```
{
```

```
    extraa[i] = R_1[ extend[i]-1 ];
```

```
}
```

```
for( int i=0; i<keyy.length(); i++ )
```

```
{
```

```
    if( extraa[i]==keyy[i] )
```

```
        anss += "0";
```

```
    else
```

```
        anss += "1";
```

```
}
```

```
int compress[32] = {
```

```
    1, 2, 3, 4, 5, 6, 7, 8,
```

```
    9, 10, 11, 12, 13, 14, 15, 16,
```

```
    17, 18, 19, 20, 21, 22, 23, 24,
```

```
    25, 26, 27, 28, 29, 30, 31, 32
```

```
};
```

```
compressed = mess_bin.substr(0, 32);
```

```
for( int i=0; i<32; i++ )
```

```
{
```

```
    compressed[i] = anss[ compress[i]-1 ];
```

```
}
```

```
return compressed;
```

```
}
```

```
int main()
```

```
{
```

```
    init();
```

```
    string key_final, key_bin, key_after_PC1, CO, DO, comb_str, key_after_PC2,  
    LO, RO, anss = "";
```

```
    string extraa, compressed, LO_xor_comp = "", rev_comb, ip_inv, hex = "",  
    leff, righ, RO_xor_comp = "";
```

```
    string bin_decr, hexii = "";
```

```
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
```

```
// :::Generating Round Keys::: //
```

```
key_bin = to_binary("24648A5B9DB4E560");
```

```
/*
```

Since DES uses key of 56 bits, we will apply PC1 on 64 bit key. So, lets drop every

8th bit in 64 bits message, and then put in reverse order.

Let the PCI table be:

```
*/
```

```
int PC1[56] = {
```

```
    63, 55, 47, 39, 31, 23, 15, 7,
```

```
    62, 54, 46, 38, 30, 22, 14, 6,
```

```
    61, 53, 45, 37, 29, 21, 13, 5,
```

```
    60, 52, 44, 36, 28, 20, 12, 4,
```

```
    59, 51, 43, 35, 27, 19, 11, 3,
```

```

58, 50, 42, 34, 26, 18, 10, 2,
57, 49, 41, 33, 25, 17, 9, 1
};

```

```

/*

```

This means 63rd bit becomes 1st bit, 55th bit becomes 2nd bit and so on..

```

*/

```

```

key_after_PC1 = key_bin.substr(0, 56);

```

```

for(int i=0; i<56; i++)

```

```

{

```

```

    key_after_PC1[i] = key_bin[ PC1[i]-1 ];

```

```

}

```

```

CO = key_after_PC1.substr(0, 28);

```

```

DO = key_after_PC1.substr(28, 28);

```

```

/*

```

Applying LSH on CO and DO.(Left shift by 1)

```

*/

```

```

CO = LSH( CO );

```

```

DO = LSH( DO );

```

```

comb_str = CO + DO;

```

```

/*

```

We will apply PC2 on 56 bit key to form 48 bits. So, lets drop every 8th bit in 56 bits

message plus 55th and 56th bit, and put in correct order.

Let the PC2 table be:

```
*/
```

```
int PC2[56] = {  
    1, 2, 3, 4, 5, 6, 7, 9,  
    10, 11, 12, 13, 14, 15, 17, 18,  
    19, 20, 21, 22, 23, 25, 26, 27,  
    28, 29, 30, 31, 33, 34, 35, 36,  
    37, 38, 39, 41, 42, 43, 44, 45,  
    46, 47, 49, 50, 51, 52, 53, 54  
};
```

```
key_after_PC2 = key_bin.substr(0, 56);
```

```
for(int i=0; i<56; i++)
```

```
{  
    key_after_PC2[i] = comb_str[ PC2[i]-1 ];  
}
```

```
key_final = key_after_PC2;
```

```
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
```

```
cout << "Message: " << endl;
```

```
mess_bin = to_binary("4A8260748070636E");
```

```
cout << "In binary: " << mess_bin << endl;
```

```
cout << "In hexadecimal: " << "4A8260748070636E" << endl;
```

```
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
```

```
cout << "Encryption: " << endl;
```

```
LO = mess_bin.substr(0, 32);
```

```

RO = mess_bin.substr(32, 32);

compressed = f_function(RO, key_final); // RO xor key_final
for( int i=0; i<LO.length(); i++ )
{
    if( compressed[i]==LO[i] )
        LO_xor_comp += "0";
    else
        LO_xor_comp += "1";
}
LO = RO;
RO = LO_xor_comp;

rev_comb = RO + LO;

for(int i=0; i<(int)rev_comb.length(); i+=4)
{
    string gh = rev_comb.substr( i, 4 );
    hex += ma_rev[gh];
}
cout << "In binary: " << rev_comb << endl;
cout << "In hexadecimal: " << hex << endl;

////////////////////////////////////////////////////////////////

////////////////////////////////////////////////////////////////

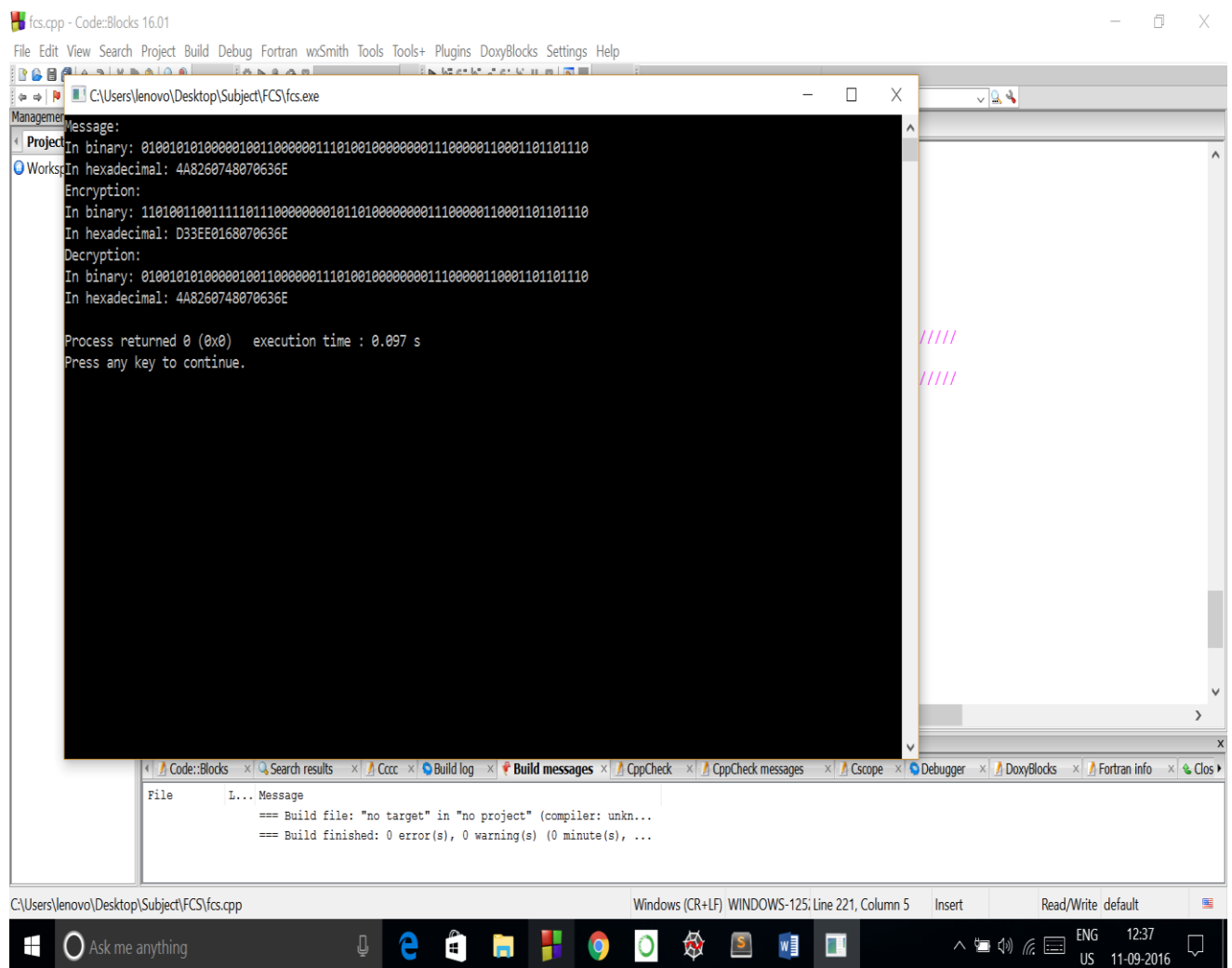
cout << "Decryption: " << endl;

```


[illegible]

*/

Output:



```
fcs.cpp - Code::Blocks 16.01
File Edit View Search Project Build Debug Fortran wxSmith Tools Tools+ Plugins DoxyBlocks Settings Help
C:\Users\lenovo\Desktop\Subject\FCS\fcs.exe
Message:
In binary: 010010101000001001100000011101001000000011100000110001101101110
In hexadecimal: 4A8260748070636E
Encryption:
In binary: 1101001100111110111000000001011010000000011100000110001101101110
In hexadecimal: D33EE0168070636E
Decryption:
In binary: 010010101000001001100000011101001000000011100000110001101101110
In hexadecimal: 4A8260748070636E

Process returned 0 (0x0)   execution time : 0.097 s
Press any key to continue.

==== Build file: "no target" in "no project" (compiler: unkn...
==== Build finished: 0 error(s), 0 warning(s) (0 minute(s), ...

C:\Users\lenovo\Desktop\Subject\FCS\fcs.cpp  Windows (CR+LF)  WINDOWS-1251, Line 221, Column 5  Insert  Read/Write: default  ENG 12:37 11-09-2016
```

Ans 5).

The guards at IIIT Delhi allow anyone to enter the college premise as long as they enter their details in a Ledger.

For usability this procedure has advantage that if a student forgets his ID card, he can easily come in college by entering his details in the Ledger. Secondly, if a parent or any friend of the student wants to visit the campus and meet the person, they can easily do so without much hassle. This makes life convenient.

However if we see from security point of view then it is not much safe. These details cannot authorise, authenticate and identify that the person is not an anti-social element. The person who is entering details may not be an anti-social element. Those details may not be correct and guards may end up allowing anti social element inside the campus. No frisking or checking correctness of details can become costly one day.

If I were to propose an altering solution for entering the college, I would look out for any of these: driving licence, ID card of the company he is working for, PAN card, Aadhar Card, etc. which uniquely identify the person. So instead of directly mentioning just on a Ledger, it would be better to verify the details of the person through any of the above cited document. Since most people come via their transport, most of them would be carrying their driving licence and thus it would suffice the purpose. So it's quite usable as there is just one check to verify identity of the person. Secondly, proper frisking can be done of suspicious person. This method would not only be secure but also usable. These details authorise, authenticate and identify the person uniquely.

By:

Deepak Thukral