Cryptology Assignments

Jamie Southgate

Honours Degree
University of the Western Cape
2016

Declaration

I declare that this assignment was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*Jamie Southgate*)

Contents

Assignment 1

1.1a Symmetric Encryption

Symmetric Encryption involves the use of a key which is used to encrypt and decrypt the message. The key is therefore used by both the sender and receiver. For example, Alice wants to send a secret message to Bob. This is the plaintext. The message then needs to be encrypted with a key so only Bob can read the message. This encrypted message is called a ciphertext. Bob receives the ciphertext, knowing the key to use the same symmetric cipher to decrypt the message. Alice and Bob undertake the same encrypt/decrypt process which is a symmetric process.

1.1b Asymmetric Encryption

Asymmetric Encryption involves the use two related keys, a public and private key. The public key is available for everyone but the private key is only known by the trusted recipient. The public key is used to encrypt the message and can only be decrypted by the corresponding private key. Asymmetric ciphers are slow compared to symmetric ciphers. By using asymmetric ciphers to distribute the key, Alice and Bob can use a symmetric cipher to communicate securely.

1.1c Multiple Encryption

Multiple Encryption is the process of encrypting an already encrypted message once or multiple times using the same or different algorithms.

1.1d Three-way pass protocol

The three-way pass protocol enables users to communicate privately without exchanging or distributing encryption keys. It is based on commutative encryption whereby each user has a private encryption and decryption key. Alice sends Bob an encrypted message. Bob receives the message and encrypts it with his own encryption key and sends it back to Alice. Alice then decrypts the message and sends it back to Bob. When Bob receives the message he then decrypts the message using his decryption key and then the message is readable. The reason why the three-way pass can be insecure is that the same message is exchanged three times and therefore more vulnerable interception.

1.2 Vernam cipher

Plaintext: Wieniawski
Cipher: Zymanowski

Table 1.1:

DEC ASCII code	Cipher	Addition	MOD(127)
87	90	177	50
105	121	226	99
101	109	210	83
110	97	207	80
105	110	215	88
97	111	208	81
119	119	238	111
115	115	230	103
107	107	214	87
105	105	210	83

Table 1.2: Binary Output

7-bit ASCII code	7-bit Cipher	XOR
1010111	1011010	0001101
1101001	1111001	0010000
1100101	1101101	0001000
1101110	1100001	0001111
1101001	1101110	0000111
1100001	1101111	0001110
1110111	1110111	0000000
1110011	1110011	0000000
1101011	1101011	0000000
1101001	1101001	0000000

Decimal Integer Stream Ciphertext: 5099838088811111038783

Bit Stream Ciphertext: 00011010010000000100000011110000111000111000000000000000000000000000000

Alphanumeric Stream Ciphertext: 2cSPXQogWS

1.3 Vernam cipher and Information Entropy

The reason why additive based encryption methods reduce information entropy is because of varying bits of values i.e., suppose we wish to encrypt Hello World, we might find that the ordinal value 2 of each character in the plain-text have different bit lengths so W might have bit length 6 while e has bit length 4. It is for this reason that we require to use one-time pad. One-time pad allows us to force each ordinal value of each character in the plain-text to be the same bit length.

Assignment 2

2.1a Hash Function

A hash function is a one way function that takes in an input and returns a string output that is fixed in size.

2.1b Cycle Length

The cycle length is the amount of data in a cipher stream before the stream repeats itself.

2.1c Maximum Entropy Cipher

Entropy is the planned disorder given to the set of cipher-text in a message.A maximum entropy cipher is one that distorts the cipher-text as much as possible to eliminate any structure.

2.1d Crib

A crib is a segment of an encrypted message that can easily be restored into plain text.

2.2a Hash Function Code - Key

```
def Hash(PIN):
    a = random.randrange(2**16) #x^a
    b = random.randrange(2**16) #bx
    c = random.randrange(2**16) #c
    prime = 2**32-1
    offshoot = 1234
    if (0 < PIN < 9999 ):
        PIN = ((PIN**a)+(PIN*b)+c)%prime #Quadratic Function
        key = ((prime*PIN)+offshoot)
        key = key % 2**16
        return key
    return 0

print Hash(1234)
23495
```

2.3 Blum-Blum-Shub Generator

```
def BlumBlum(Key,BI,N)
    cipher = []
    x=Key
    for i in range(1,N):
        x = x**2
        cipher.append(x%BI)
    return cipher
```

Assignment 3

3.1 Matthews Cipher

```
#Matthews Cipher - r = 4
def Matthews(n, key):
    x = [key]

    r = 4

    for i in range(n - 1):
        x.append((1 + r) * (1 + (1 / r)) * x[i] * ((1 - x[i]) ** r))

    return x
```

3.2 Encrypt

```
#Reads File from Args - Encrypts input with cipher and outputs cipher text

def ENCRYPT(key):

    plaintext = open(str(sys.argv[1])).read() #Readfile

    stream = Matthews(len(plaintext),key) #Compute Mathews Cipher on line


    e = open(str(sys.argv[2]), w )

    e.write(stream)

    e.close()
```

3.3 Decrypt

```
def DECRYPT(key):
    ciphertext = open(str(sys.argv[1])).read() #Read File
    stream = MATTHEWS(len(ciphertext),key) #Cipher
    plaintext = Decipher(ciphertext,stream)
    e = open(str(sys.argv[2]), w ) #Write to Fule
    e.write(plaintext)
    e.close()
```

```
def Decipher(ciphertext,stream):
    x=[]
    for i in range(len(ciphertext)):
        info = int(ciphertext[i],2)
        confusion = int(stream[i]) #noise
        x.append(bin(info-confusion)) #remove cipher from cipher text
    return x
```

3.4 Application

```
def ENCRYPT_DECRYPT(key,option):
    if (option):
        ENCRYPT(key)
    else:
        DECRYPT(key)

    if ((len(sys.argv)==5) and (str(sys.argv[1])=="-e")):
        ENCRYPT_DECRYPT(float(sys.argv[2]),True)
    elif ((len(sys.argv)==5) and (str(sys.argv[1])=="-d")):
        ENCRYPT_DECRYPT(float(sys.argv[2]),False)
    else:
        print ("Error")
```

Assignment 4

Chaotic Cipher 1: $x_{n+1} = rx[1 - tan(\frac{x}{2})]$

Lyapunov exponent: $\sigma = \lim_{N \to 1000} \frac{1}{N} \sum_{N}^{n=1} ln(\frac{\epsilon_n + 1}{\epsilon_n}) = 0.94507$

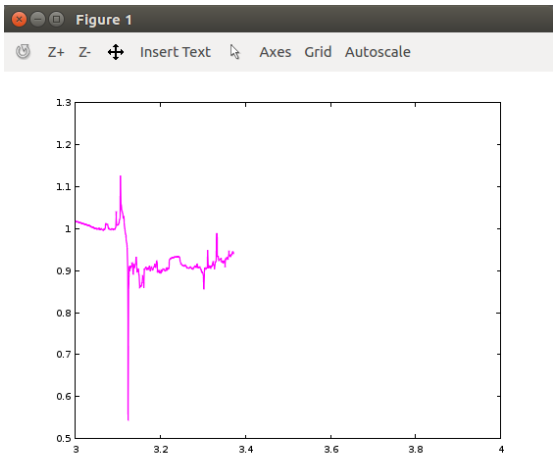

Figure 4.1: Lyapunov Exponent for variations of r

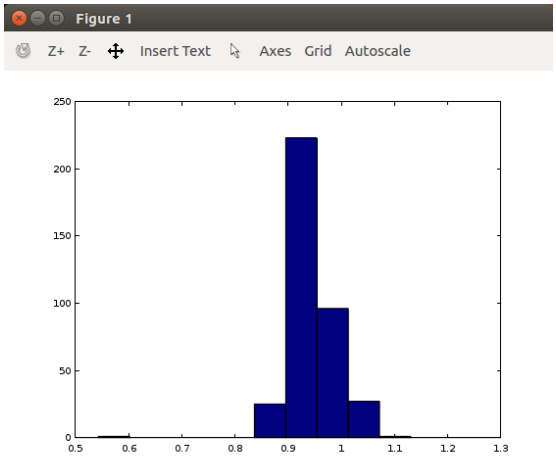

Figure 4.2: Histogram of Cipher 1

Chaotic Cipher 2: $x_{n+1} = rx[1 - sin(x^2)]$

Lyapunov exponent: $\sigma = \lim_{N \to 1000} \frac{1}{N} \sum_{N}^{n=1} ln(\frac{\epsilon_n + 1}{\epsilon_n}) = 1.04074$

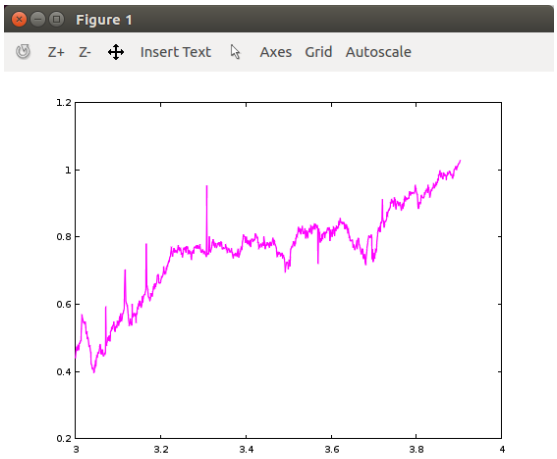

Figure 4.3: Lyapunov Exponent for variations of r

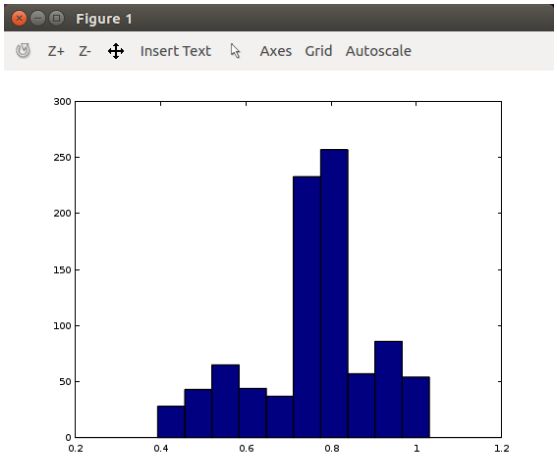

Figure 4.4: Histogram of Cipher 2

Chaotic Cipher 3: $x_{n+1} = rx[1 - log\frac{x+1}{x}]$

Lyapunov exponent: $\sigma = \lim_{N\to 1000} \frac{1}{N} \sum_{N}^{n=1} ln(\frac{\epsilon_n+1}{\epsilon_n}) = 1.3447$

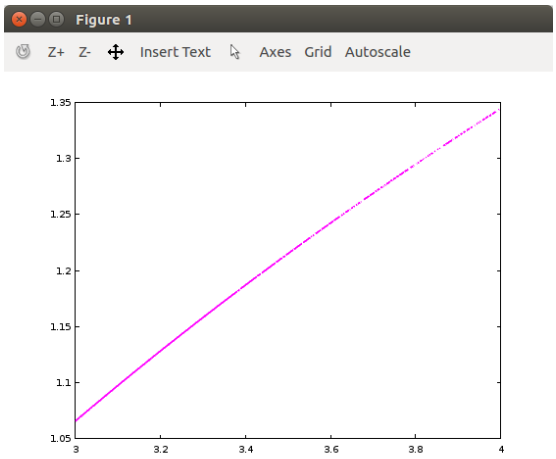

Figure 4.5: Lyapunov Exponent for variations of r

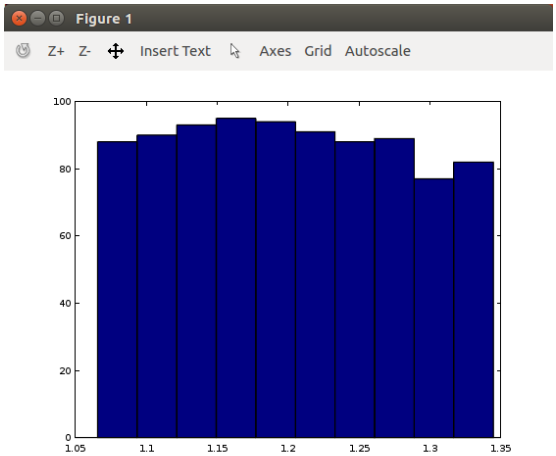

Figure 4.6: Histogram of Cipher 3

Assignment 5

5.1a Confusion

The ciphertext must depend on the plaintext and the key in a complicated way so that the derivation of statistical relations is difficult to compute. The relationship between ciphertext and key should be as complex as possible.

5.1b Diffusion

Changing one symbol in the plaintext affects many symbols in the ciphertext and changing one symbol in the key affects many symbols in the ciphertext.

5.2 Diffusion Equation

For the case when:

$$(\Delta^2 - \sigma\frac{\partial}{\partial t})u(x,t) = -S(x,t), u(x,0) = 0$$

the solution is:

$$u(x,t) = G(|x|,t) \otimes_x \otimes_t S(x,t), t > 0$$

.
Let

$$S(x,t) = s(x)\delta(t)$$

then the solution is given by

$$u(x,t) = G(|x|,t) \otimes_x s(x), t > 0$$

Observe that

$$u(x,0) = u_0(x)$$

thus

$$u(x,t) = G(|x|,t) \otimes_x [s(x) + u_0(x)] = G(|x|,t) \otimes_x u_0(x) + n(x,t), t > 0$$

where

$$n(x,t) = G(|x|,t) \otimes_x s(x)$$

If s is a stochastic function then n is a stochastic function and its inverse is as follows.
Suppose:

$$D\Delta^2 u(x,t) - \frac{\partial}{\partial t}u(x,t) = 0, u(x,0) = u_0(x)$$

with solution:

$$u(x,t) = \frac{1}{D} G(|x|,t) \otimes_x u_0(x), t > 0$$

We can express $u(x,0)$ in terms of $u(x,T)$ using the Taylor series

$$u_0(x) \equiv u(x,0) = u(x,T) + \sum_{n=1}^{\infty} \frac{(-1)^n}{n!} T^n \left[\frac{\partial^n}{\partial t^n} u(x,t) \right]_{t=T}$$

Now from the diffusion equation

$$\frac{\partial^2 u}{\partial t^2} = D\Delta^2 \frac{\partial u}{\partial t} = D^2 \Delta^4 u$$

$$\frac{\partial^3 u}{\partial t^3} = D\Delta^2 \frac{\partial^2 u}{\partial t^2} = D^3 \Delta^6 u$$

Thus in general we can write:

$$\left[\frac{\partial^n}{\partial t^n} u(x,t) \right]_{t=T} = D^n \Delta^{2n} u(z,y,T)$$

Substituting this result into the series for u_0 given above, we obtain

$$u_0(x) = u(x,T) + \sum_{n=1}^{\infty} \frac{(-1)^n}{n!} (DT)^n \Delta^{2n} u(x,T)$$

5.3 Stochastic Function

5.4 Watermark

```
function watermark(cipher,plaintext,covertext,sz,R)
    code=cipher; %Cipher = 1234
    pt = imread(plaintext); %Read plaintext
    ct = imread(covertext); % Read Covertext

    pt = im2double(pt);
    ct = im2double(ct);

    pt = 1-pt; %watermark


    size = size(pt,1) %Get Size
    rand('state',code); %Generate Random
    noise = rand(size,size); %Noise Creation
    %Display
    subplot(2,3,1),imshow(pt);
    subplot(2,3,2),imshow(ct);
    subplot(2,3,3),imshow(noise);

    cipher = fft2(noise); %Compute spectrum of cipher
    plaintext = fft2(pt); %Compute the spectrum of plaintext
    powerspectrum = abs(noise).^2; %Compute Power Spectrum
    for i=1:size %Preconditon power spectrum of cipher
      for j=1:size
        temp=powerspectrum(i,j);
        if temp==0
```

```
      powerspectrum(i,j)=1;
     else
      powerspectrum(i,j)=powerspectrum(i,j);
    end
  end
end
%Diffuse plaintext image with pre-conditioned cipher
plaintext = plaintext(:,:,1);
plaintext=cipher.*plaintext./powerspectrum;

plaintext = ifft2(plaintext);
plaintext = real(plaintext); %Compute real part of IFFT
plaintext = plaintext./max(max(plaintext)); %Normalise diffusion

subplot(2,3,4),imshow(plaintext,[min(min(plaintext)) max(max(plaintext))])

%Compute Watermark
covertext = ct(:,:,1);
watermark = R*plaintext+covertext;
subplot(2,3,5), imshow(watermark)

%Subtract covertext from watermaked image
diffusion = watermark - plaintext;

diffusion = diffusion./max(max(plaintext)); %normalize
plaintext = diffusion;
plaintext=fft2(plaintext); %compute spectrum of diffusion field
rand('state',code);
cnoise = rand(size,size);
cnoise = fft2(cnoise); %compute spectrum of cipher
plaintext = conj(cnoise).*plaintext; %correlate diffused field with cipher
plaintext=ifft2(plaintext);
plaintext = real(plaintext) %compute real part of IFT
plaintext=plaintext./max(max(plaintext)); %normalize
subplot(2,3,6),imshow(plaintext,[min(min(plaintext)) max(max(plaintext))]) %display
```

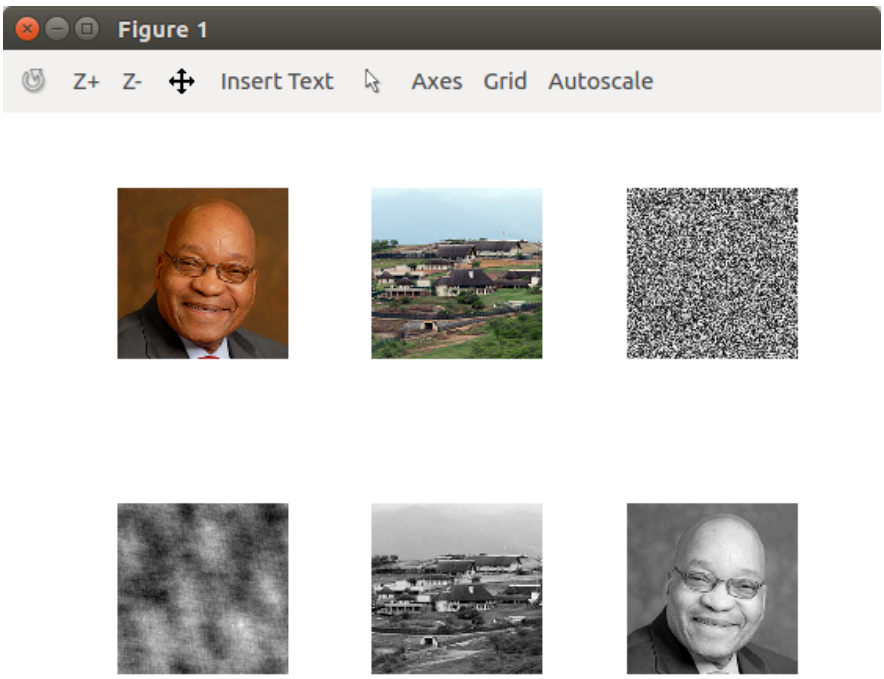

Figure 5.1: Screenshot showing Watermark, host image and cipher followed by diffused image, host image after watermarking and the recovered watermark.

Assignment 6

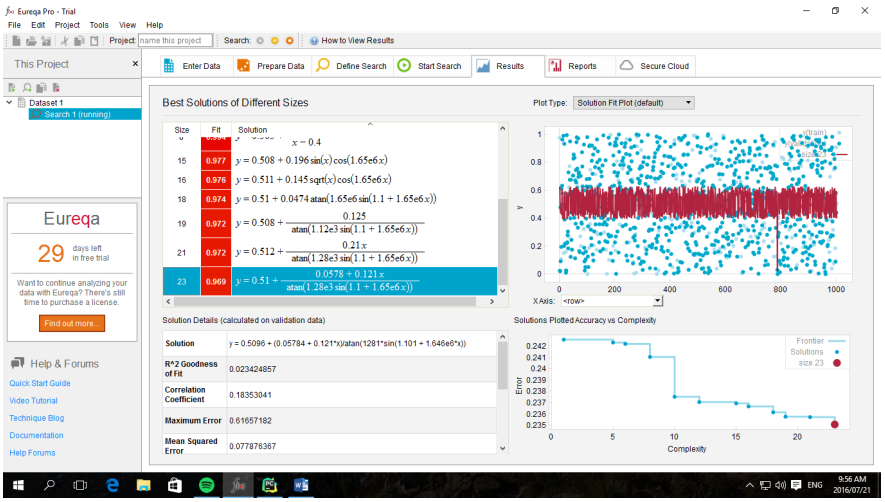

Figure 6.1: Screenshot of Eureqa - Cipher and Data

Cipher: $y = 0.51 + \frac{0.0578+0.121x}{arctan(1.28e3sin(1.1+1.65e6x))}$

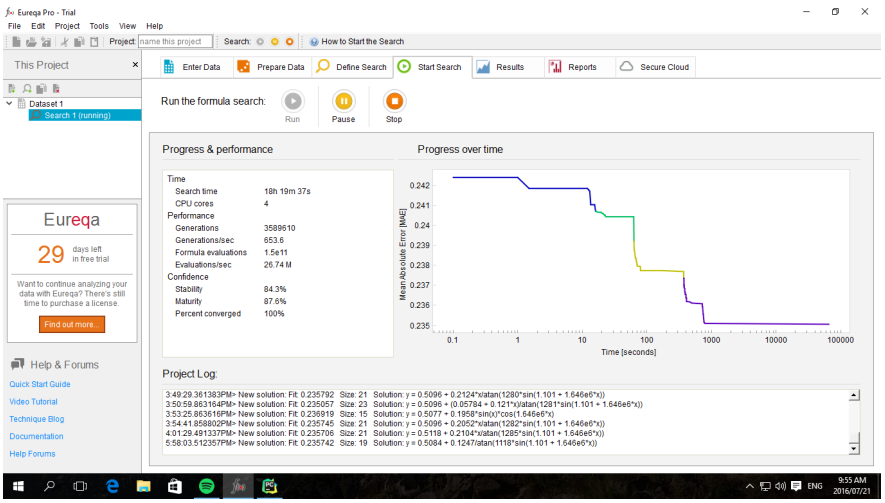

Figure 6.2: Screenshot of Eureqa -Stability and Maturity

Stability:84.3%
Maturity:87.6%

Assignment 7

Introduction
Cloud computing is the delivery of on-demand computing resources such as processing power and data over the internet. With the substantial increase in data transfer in recent years, especially in regards to sensitive information, data security has become a key focus area. The Cloud Security Alliance provides recommendations to reducing risk when adopting cloud computing outlined in their paper Security Guidance for Critical Areas of Focus in Cloud Computing. Data Security involves the use of specific controls and technologies to enforce information governance. This essay summarizes the critical areas of focus in regards to securing data on the cloud.

Content Discovery
Content Discovery is the processes and tools that are used to identify information in storage in regards to sensitivity and to define policies based on data type, structure, location and policy violations. The main use of content discovery is to help prevent data loss which is critical in securing data.

Incident Response
There are various methods with regards to preventative security controls but this does not eliminate the possibility of an attack. Incident Response is the corner stone of data security and involves the efficient and effective handling of a response to an attack on data in the cloud. The incident response lifecycle is a framework that can be used in response to attacks. It involves a three step process of preparation, detection and analysis, and containment, eradication and recovery.

Encryption
Encryption is the process of encoding information so that it can be read only by authorized users. Encryption systems normally consist of one or more algorithms that are computationally difficult to break. Its application varies amongst the three main areas of cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

In IaaS encryption, volume storage encryption is used to protect volumes from risks such as snapshot cloning, cloud provider exploration and physical loss of drives. IaaS drives can be encrypted using externally managed encryption where the encryption engine runs in the instance but the keys are managed externally and issued to the instance on request.

PaaS has many potential options regarding encryption. Client/application encryption can be used to encrypt the data in the PaaS application or client accessing the platform. Database encryption can also be used to encrypt data in the database as well as Proxy encryption to pass data through an encryption proxy before being sent to the platform.

SaaS encryption may use any of the previously discussed options for encryption. Provider-managed encryption is another option for SaaS users whereby data is encrypted in the SaaS application and is normally managed by the provider.

Conclusion

Much progress has been made in regards to securing data on the cloud especially in terms of data governance. The growth of cloud platforms in recent years has meant an increased risk of security breaches. The risk tolerance for data assets should be evaluated in order to apply suitable encryption schemes for the deployment. Not all cloud deployments need evert possible security and risk control.

Word Count: 503