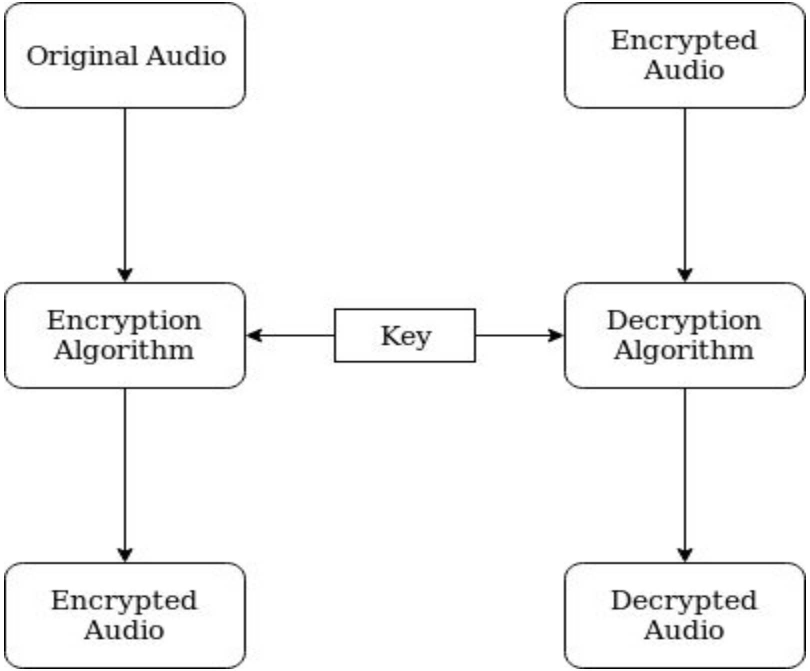
Motivation

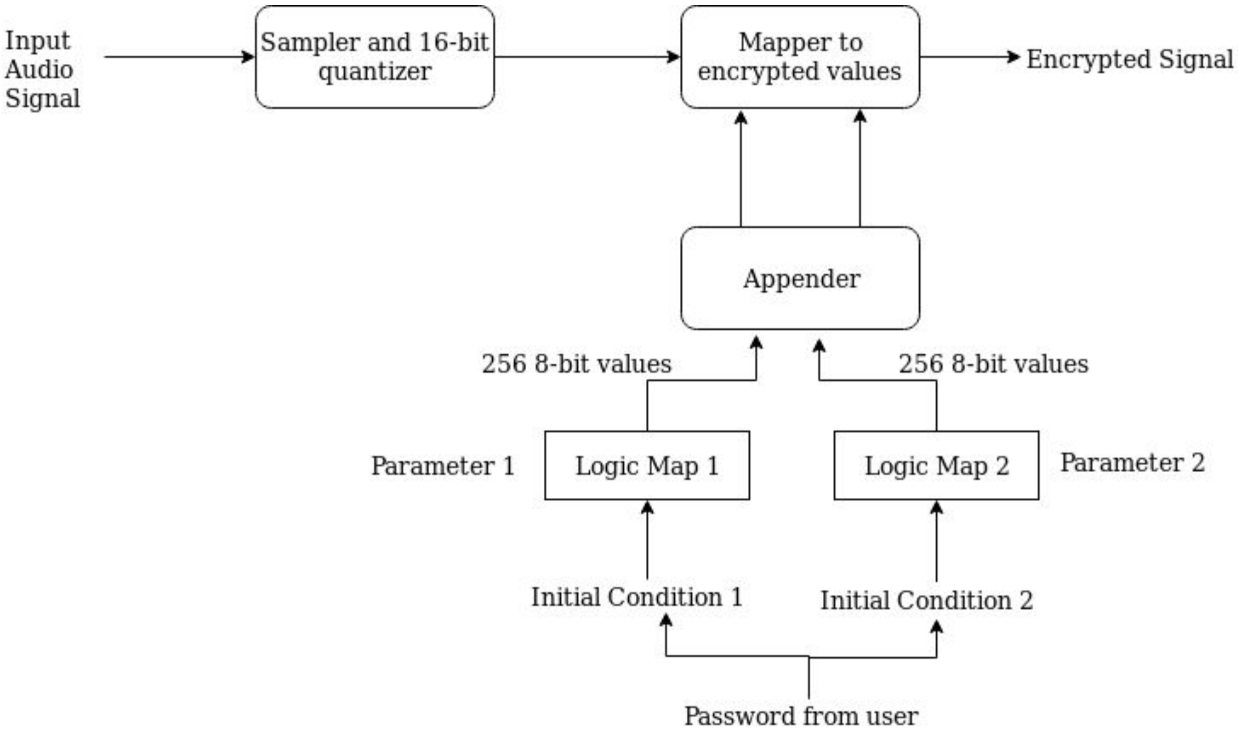
- With the dawn of the digital era privacy has become very critical.
- Today, vast amounts of personal information are managed online and stored in the cloud or on servers with an ongoing connection to the web.
- To protect this information from getting misused, various techniques such as encryption is necessary.

Introduction

- Encryption enhances the security of a message or file by scrambling the content.
- It is the most effective way to hide communication via encoded information where the sender and the recipient hold the key to decipher data.
- Mobile phones have limited computing power, hence the audio encryption scheme should faster and less complex.
- The audio encryption scheme should be complex enough and unbreakable.


Original Audio
Encrypted Audio
Encryption Algorithm
Key
Decryption Algorithm
Encrypted Audio
Decrypted Audio

Encryption Algorithm

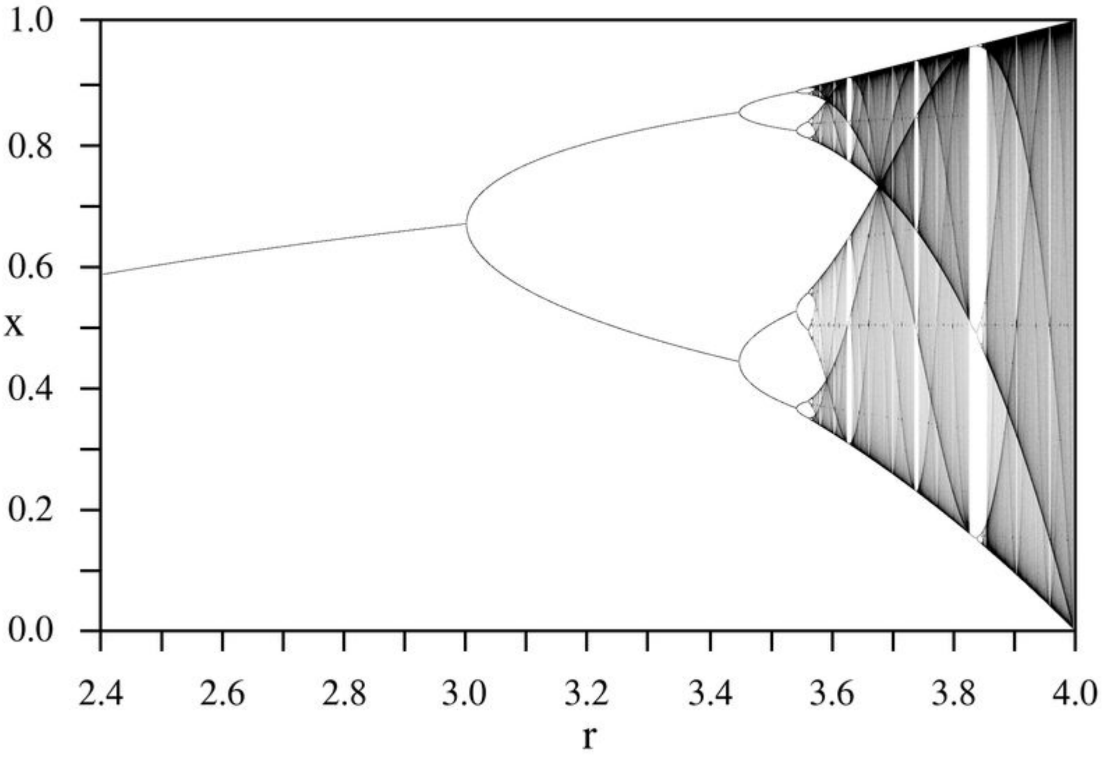


Chaotic Systems

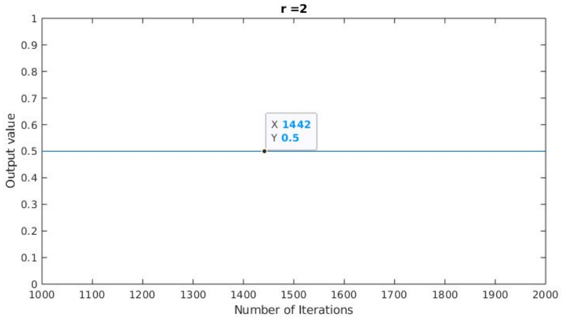
- A chaotic system is a nonlinear deterministic dynamical system which exhibits pseudorandom behaviour.
- The output values of chaotic systems vary depending on specific parameters and initial conditions.
- The encryption algorithm uses 1-D chaotic map called logistic map. The equation is as follows :

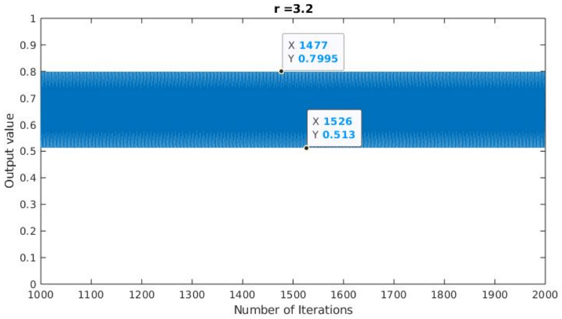
$$x_{n+1} = r\,x_n\,(1 - x_n) \qquad 0 < x_n < 1,\ 0 < r < 4$$

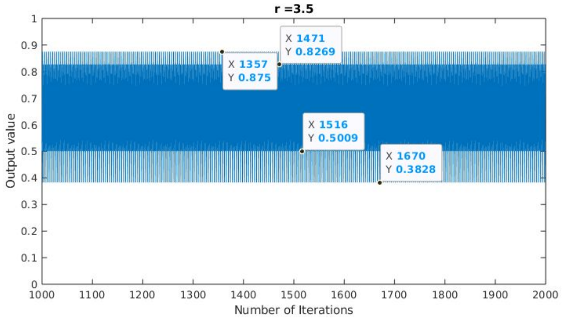
Bifurcation plot of Chaotic map

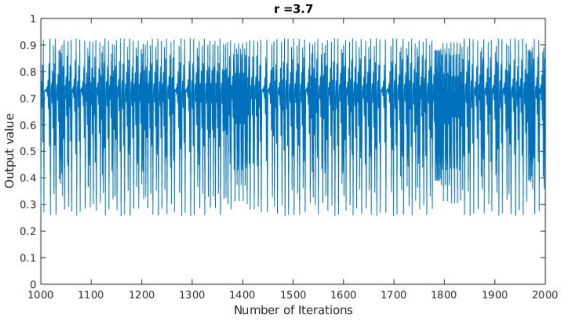


Chaotic Maps

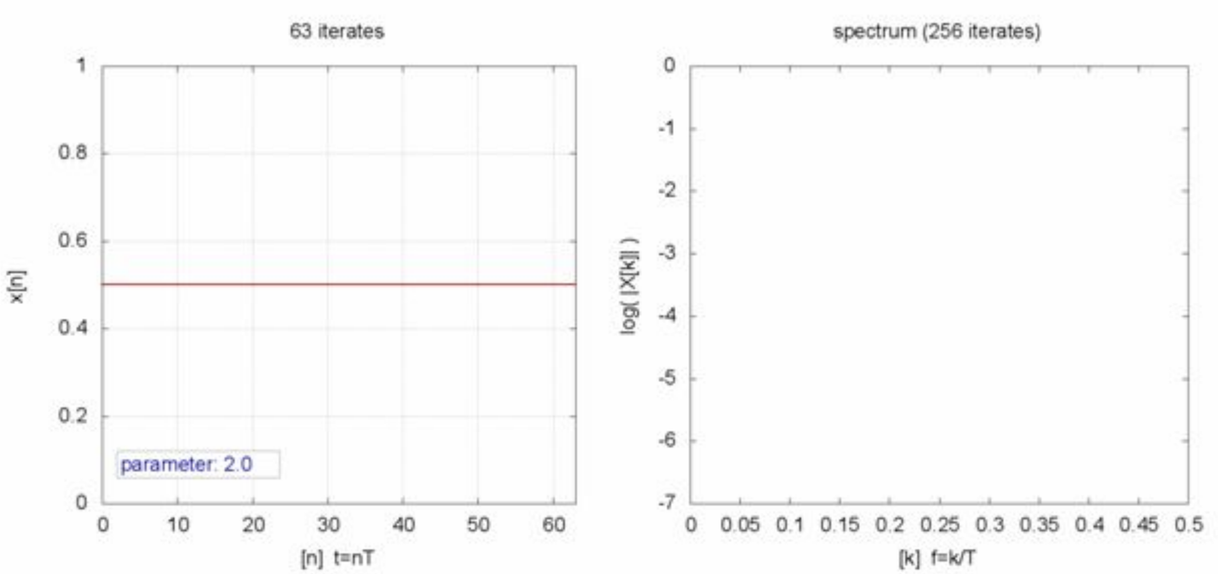








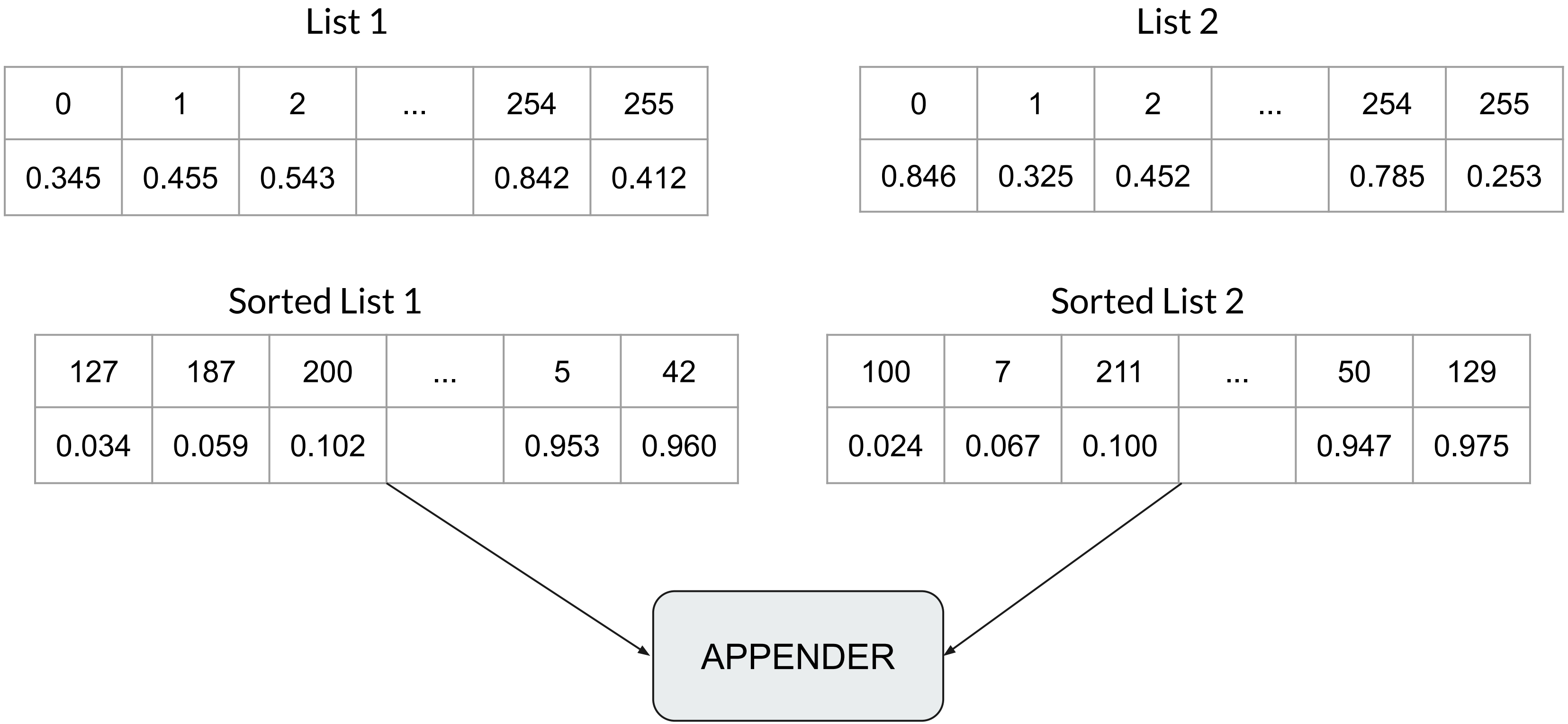
Visualization of Logistic map



Initial values x_0 and y_0

```
Function (x0, y0) = get_init_vals(password):

    Sum1, Sum2 = 0

    For a in ascii(password):

        Sum1 = (Sum1 * 31) + a

        Sum2 = (Sum2 * 37) + a

    x0 = Sum1 / max(type(Sum1))

    y0 = Sum2 / max(type(Sum2))
```

Dictionary Generation



List 1

0	1	2	...	254	255
0.345	0.455	0.543		0.842	0.412

List 2

0	1	2	...	254	255
0.846	0.325	0.452		0.785	0.253

Sorted List 1

127	187	200	...	5	42
0.034	0.059	0.102		0.953	0.960

Sorted List 2

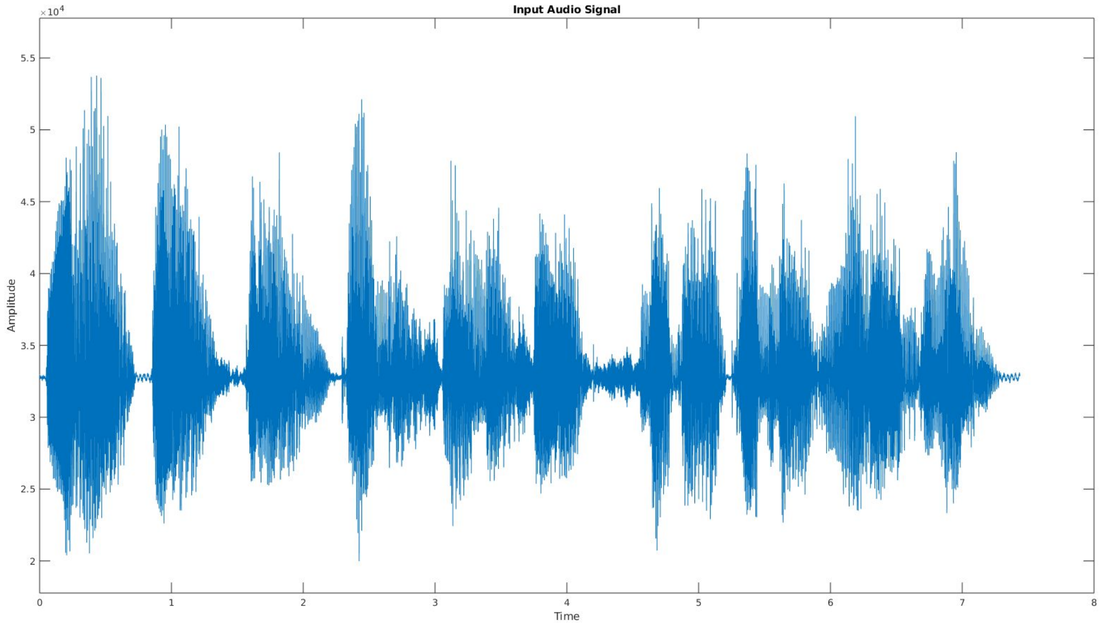
100	7	211	...	50	129
0.024	0.067	0.100		0.947	0.975

APPENDER

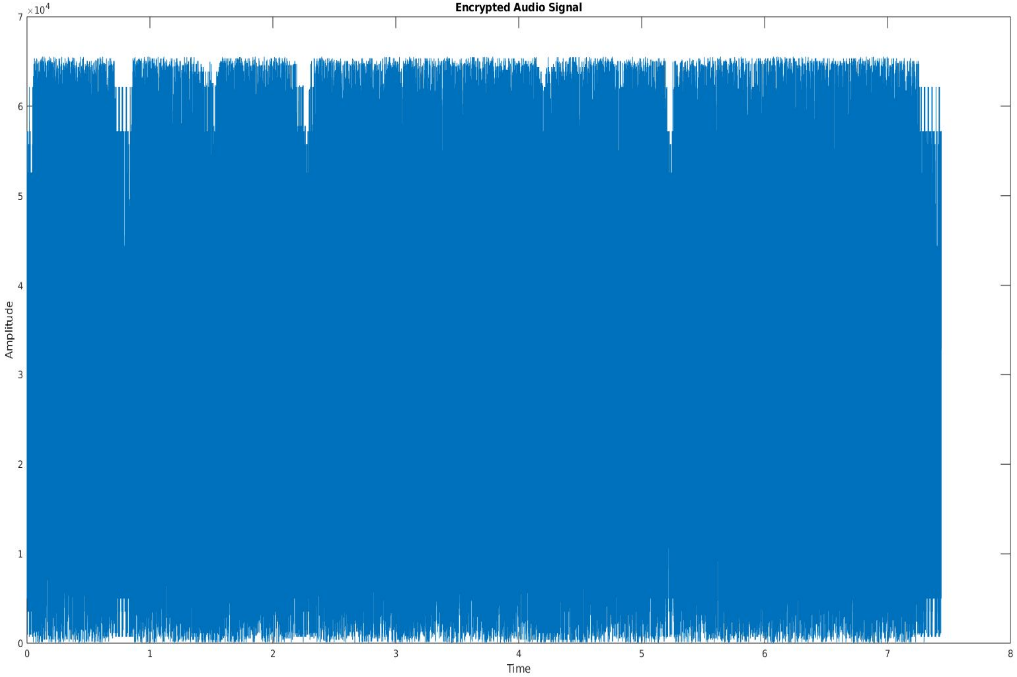
Dictionary

0	1	2	3	4	...	...	65533	65534	65535
5001	61033	23549	321	23	...	...	100	7491	9

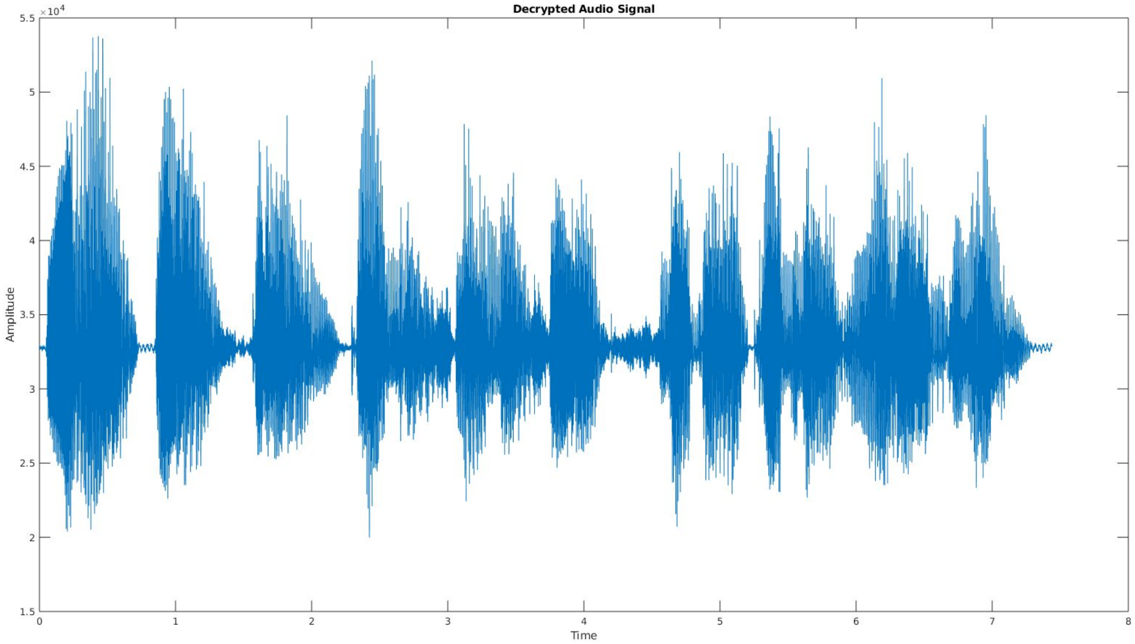
Input signal



Encrypted Signal (r1 = 3.81, r2 = 3.9, pass = “pass”)



Decrypted Signal



Thank You