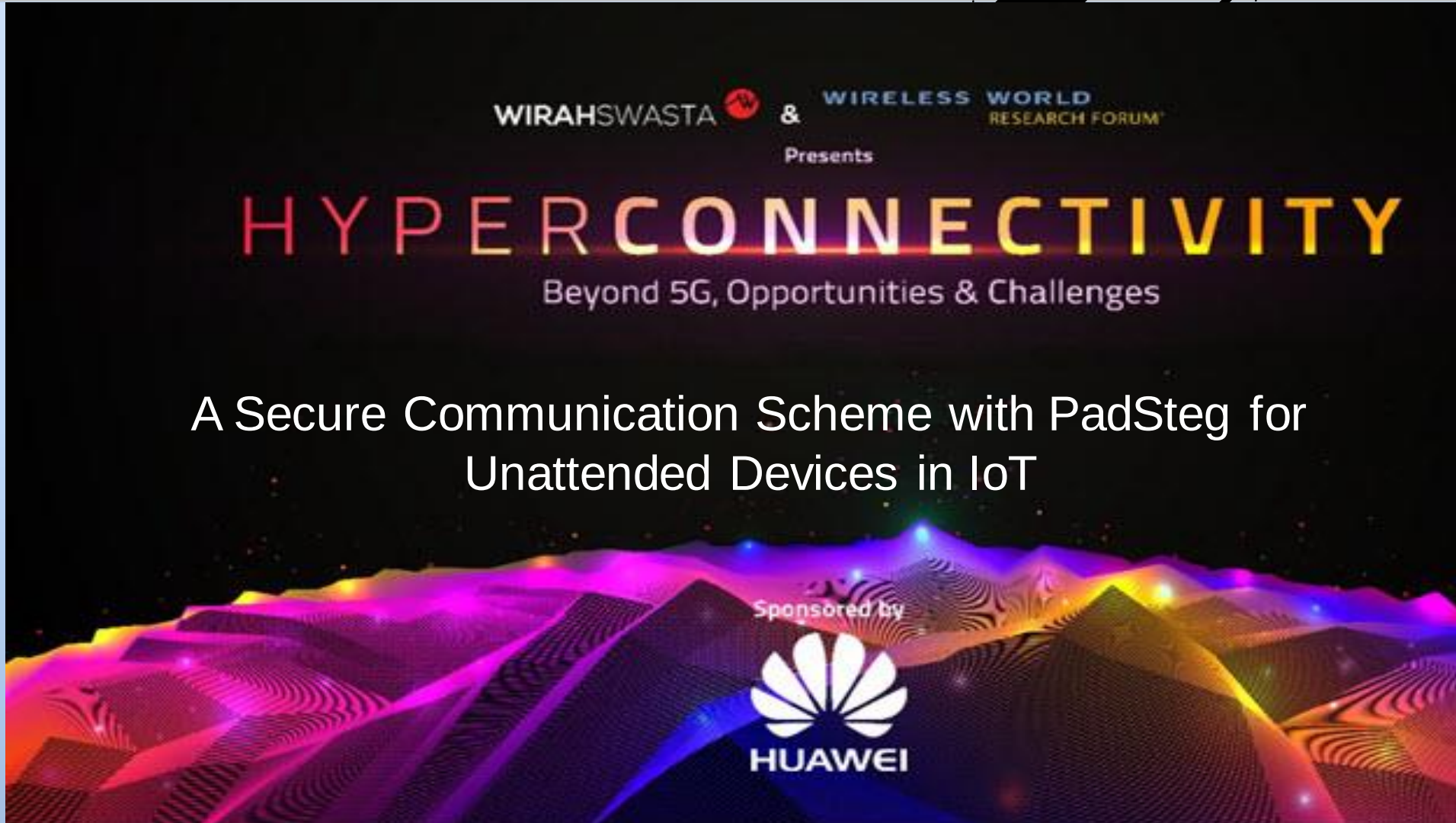

WIRAHSWASTA
&
WIRELESS WORLD
RESEARCH FORUM
Presents
HYPERCONNECTIVITY
Beyond 5G, Opportunities & Challenges
A Secure Communication Scheme with PadSteg for Unattended Devices in IoT
Sponsored by
HUAWEI

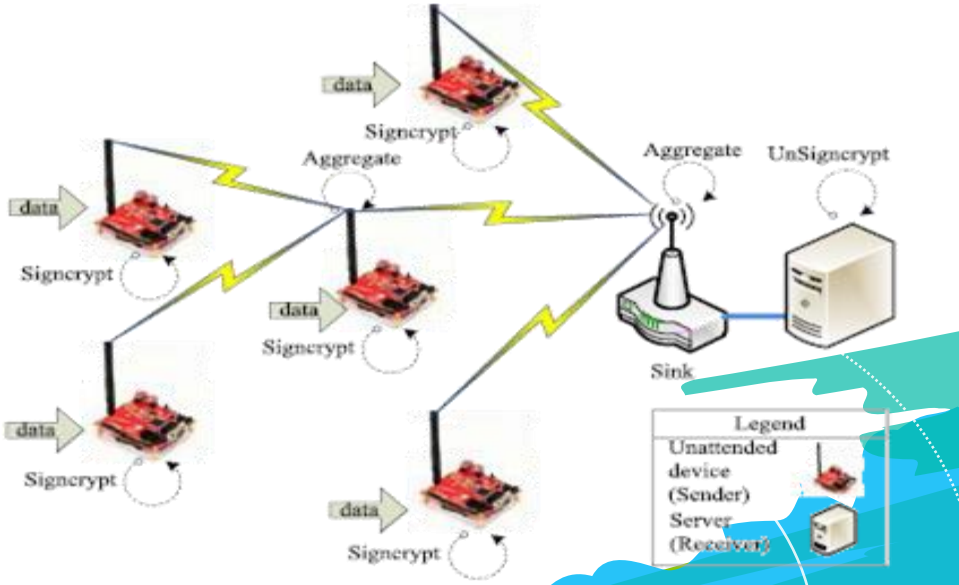
The Presenter

Inyama Victor. U
Student

Table of Content

- ❑ Introduction
- ❑ Defining IoT
- ❑ A look at the component of an IoT system
- ❑ security isuese in communication
- ❑ how to solve security Issues in IoT with SOS
- ❑ Conclusion

The Internet of Things (IoT) is the network of physical objects embedded with electronics, software, sensors, and network connectivity which enable these objects to collect and exchange data



Introduction

The IoT System

A look at the components of an IoT System

IoT Components	
Software	
Hardware	
Sensor	Communications

Issues in IoT system

1 flexibility
2 integration
3 physical Access
4 security
5 privacy
6 limited processing power & memory
7 scalability,
8 ethics communication mechanism

Physical Access

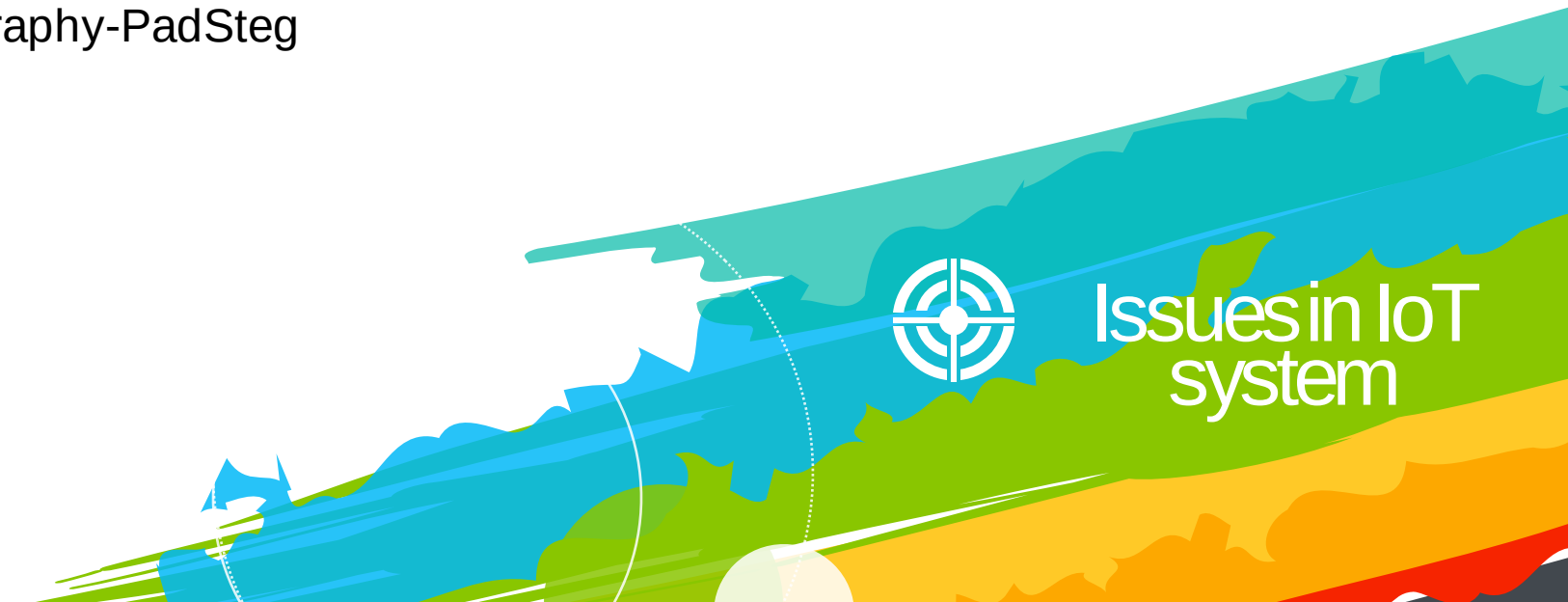
Issues in IoT system

Privacy

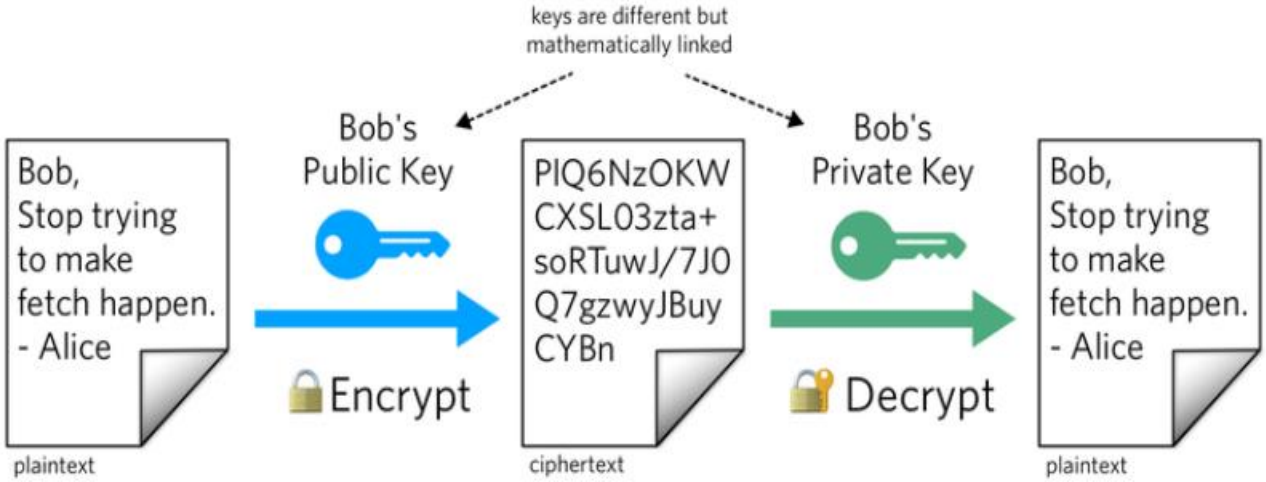
Issues in IoT system

IoT Security

1 Signcryption
2 Aggregatable signcryption
3 obfuscation
4 Stegnography-PadSteg

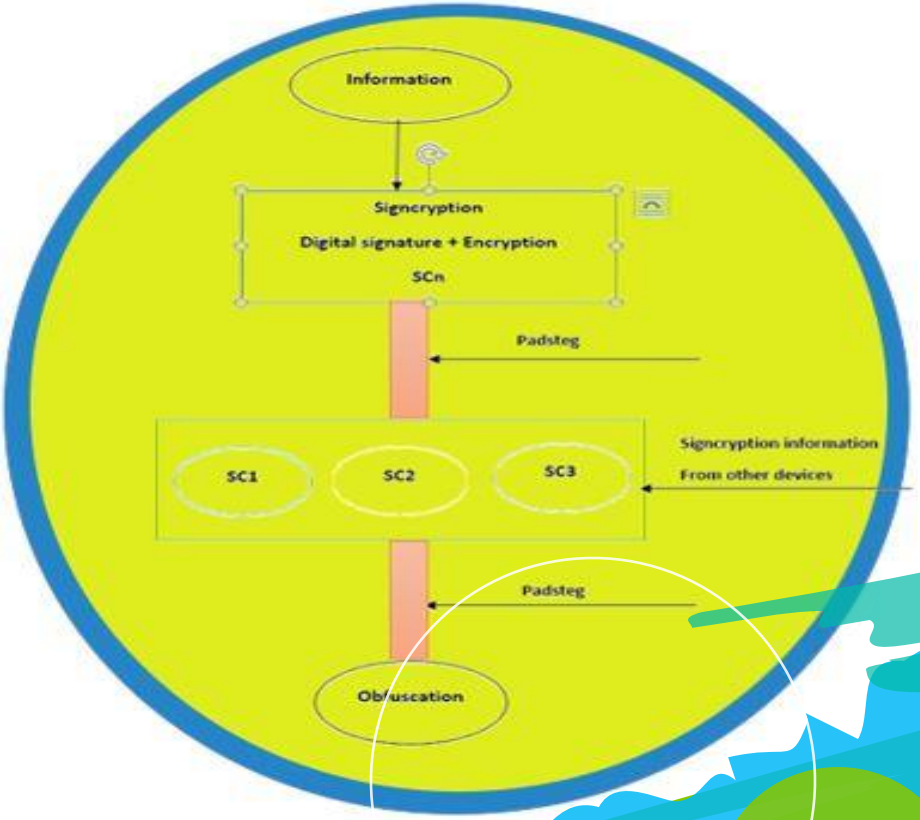


Signcryption



IoT Security

Aggregatable signcryption



IoT Security

Stegnography-PadSteg

Padding

- If one byte of padding is needed, use **01**
- If two bytes of padding are needed, use **0202**
- If three bytes of padding are needed, use **030303**
- ...
- If fifteen bytes of padding are needed, use **0f0f0f0f0f0f0f0f0f0f0f0f0f0f0f**
- If no bytes of padding are needed, add an entire block of sixteen chr(16) characters, or **10101010101010101010101010101010**

- The last byte of the plaintext is always between '\x00' and '\10'

Obfuscation

```
function myFunc(str) {
    document.write(str);
}
var myStr = "My Code";
myFunc(myStr);
```

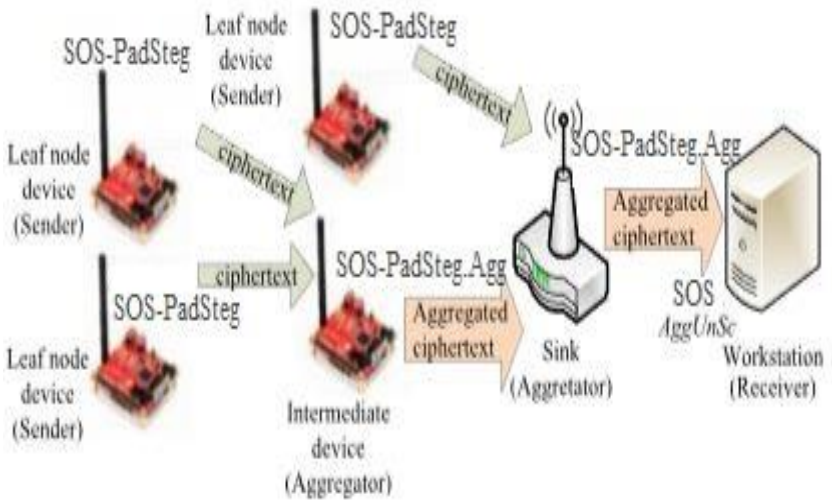
original code

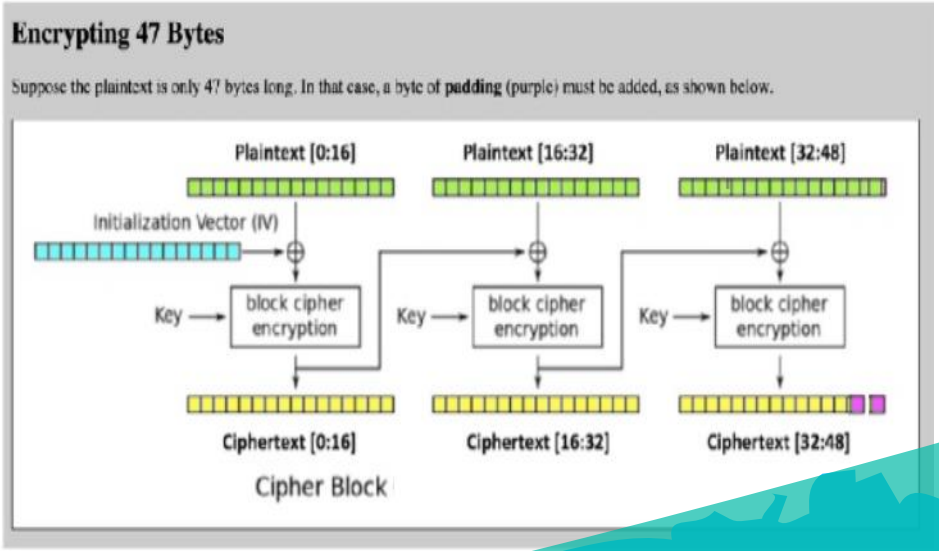
```
function msfrt23kjgty(zs12mnjy) {
    document.write(zs12mnjy);
}
var nbuqmazsuikh = "My Code";
msfrt23kjgty(nbuqmazsuikh);
```

obfuscated code

how to solve security Issues in IoT with SOS

Signcryption Obfuscatable Steganography-PadSteg (SOS) is the combination of cryptography technique such as digital signature with data encryption, obfuscation and Steganography (padding) to protect data in the IoT system. It is efficacious to protecting the confidentiality and integrity of communication in IoT environment.





Solution

Result

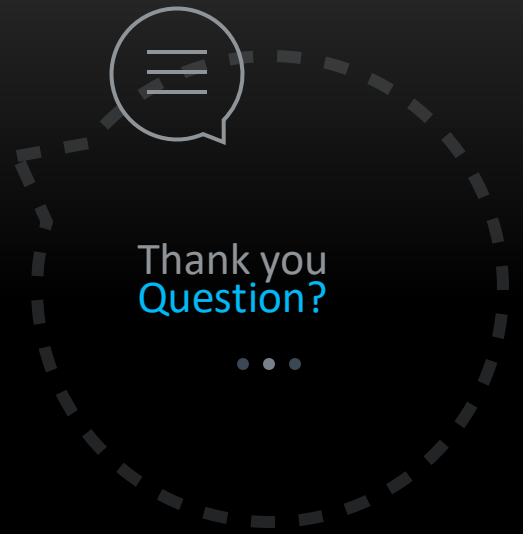
```
Enter the text:
hello mr Ali



The key is generation.... Wait.....


The Private Key is:

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAia+fM6aGSbf+jMYZ31CsjnXtCdbAhRDf+I2333nxv2hcPlF0
dHrs2+SECzlp9wX92Ml6gXfkeRWzfRRENK2g7jBkyLx9nz028t/0MOCNdwjZ8bd8
6os1MIfdGacbnsPEvdnEO6solyobA1g9UXeraxZlYUPY1DoDKLUFIGR36baUOQAj
NIQJgFbKvDb+U678MPs2kbNAdLGzPulvAkd+3WQumakL61SsFm4CSRgH2ENPRNMO
HINPxnDu5nIuOGXK6+/ZnWm3AS7U0kRj5j0ks/CxGU9rLSzlTISceloJXI8ABwln
8GkbDqpBQbRyVhZAI+P176A21/132kH3YrzMcwIDAQABAoIBAAt/Q0N8Xc1NFG/r
4OAxa99PgJYoPRY/dPxb1SVPmPy7Oayof5l0ZE/uUopfZnZOpUZTeKvT95uW0NCa
fyGI+B27o8bRWooQAgUg51KnhZiRgCV7hW5OZoghaDiKqDdHMKgLxaOX5MFOrkfG
uAQUApfkHF4VXMdH+tiM2Rs92HeG/JRfadjIZ0C84/radQ9ukX0DgR+UcCMkbDWd
jNBb8z2RuscW4ac+V7y7QQVOhNdL51Mz/MeLg+Ovh7kicBczRkZI9+DoDSz1/taL
Nz3ARS+9F0LAvd8YTpLoVlPdDRGwIVXe2mBGx9l4j2cW2HjnvrHlBUroUzzZPXYE
BjDiTjkCgYEAwsWSqgT3sra82tlkAWXIHqFEgFNuuOzum/bh19ipI78pomBANBnv
b0RNTOmdQVHu4Jv6eBTgfQvhEQI5m80i2anW9yKZNZZJWNAiKJYUzw4SFMO7JT3e
Wtrk8TBSwDtaNnWpJl6QIwnZuzO2UlUr46c6pJuBrj76MFx6GcCvSKsCgYEAtPgG
JqJnN8oh8BXLEB0wkfBQPD0eZOLupkK7P/hY+jzOw/bEafLkWYQ3mF3vG9vgt8VL
8dsujl/uRZH5sKHKGAMsGnUEYUeR7Cj1Q25OSnbd4ricaC9W4g0xTjxT6dQ4sT4Z
lZpOqOc1GuxGyzpHumnSl3pDJ6+nsbccCRhnm1kCgYBcFmlBVow5BFeiV2tB3hX
erhOzqLOzDx2AX59s9EqtB3/w1Hkj8pRWQIOdXdBtUFwcG02LfB/TYlmqB2iGZX7
Pz8AcRvraJReZ29urp1Q8t77cBlenuQrIccQe17zwFUC2ZdRK22LExIbXXQ5ckig
hKPFxDrHrMBM8rtKx3xWpwKBgBhvWN1Elm1JBLYXKzj8x/8clKjdk8oJfjHC1ue3
T8RSC5UYL8MjYnJX0O3o2Q1I7hnCMRPyBWJB/7kzeaTQ46nEW+Mio7nC4SgjC6LU
NQwG6sTfKndC1Rdmsp6etLHg7tq3yNqTYEWcGmaHOq3cK6029rFvV7v3EsyDLezo
d6zZAoGARB31TGTS6XZPSUmKdZoSDkZtoLxmrh9QzecXYQ89ZRr7jUVNoxvuQKZ9
6bj81DLTfYnkVCH3viEUhTmTw+tha6/JBhzA+PTwkNsnxuoMvR/MMA1ATUzes2d0
d7GHHcxG9xBl1a2A83Ii7GrRHkTDqzcpn1eO5v15JaA4bFvKB6k=
-----END RSA PRIVATE KEY-----


The Encryption message is:
r3VYtR7ypT0fNvUKlb4GKw==
```

```
The digital Signature is:

7734918bb2cc4c985813daba9ead21461cd27bb5c47a902b1efbbdbbce6c121ca427be1548876eb29321dff67e2
58ba449438fdd9d2ad787542856cc0c5e917c7f274c5bbc7347dd7284dda79be13ea082631b31eee6f74ac151fc
b8bc10fc73b4d95fae3abd9a3612813a9ef48b80c6e797d3e5a9429120a7e19b6fae99ed485ee8e53b2f95eac5c


The Padding Message:
hello mr Ali1111111111111111


Server Side:
------------
Check Validation the digital signature.......


Signature is Valid


The Public Key is:
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAia+fM6aGSbf+jMYZ31Cs
jnXtCdbAhRDf+I2333nxv2hcPlF0dHrs2+SECzlp9wX92Ml6gXfkeRWzfRRENK2g
7jBkyLx9nz028t/0MOCNdwjZ8bd86os1MIfdGacbnsPEvdnEO6solyobA1g9UXer
axZlYUPY1DoDKLUFIGR36baUOQAjNIQJgFbKvDb+U678MPs2kbNAdLGzPulvAkd+
3WQumakL61SsFm4CSRgH2ENPRNMOHINPxnDu5nIuOGXK6+/ZnWm3AS7U0kRj5j0k
s/CxGU9rLSzlTISceloJXI8ABwln8GkbDqpBQbRyVhZAI+P176A21/132kH3YrzM
cwIDAQAB
-----END PUBLIC KEY-----


The Decryption message is:
hello mr Ali
```

Result

Conclusion

- I have theoretically and practically proved that the SOS-PadSteg is a really good attempt to creating a network security model in IoT which ensures the confidentiality and integrity of information disseminated by nodes in IoT environment is well secured.


Thank you
Question?