Is secure communication possible?

Supervisors:
Derek Abbott
James Chappell
Lachlan Gunn

Yuanhao Liu
Christopher Lau

Outline

- Introduction
  - Is communication secure?
  - Power of eavesdroppers
  - Importance of cryptography
- Encryption
  - One time pad
  - Round trip times
- Our aims
  - The efficiency
  - The reliable
  - The speed
  - The utilisation
- Approaches
  - Software
  - hardware
- Project management
  - Risk management
  - Time management
- Question and references

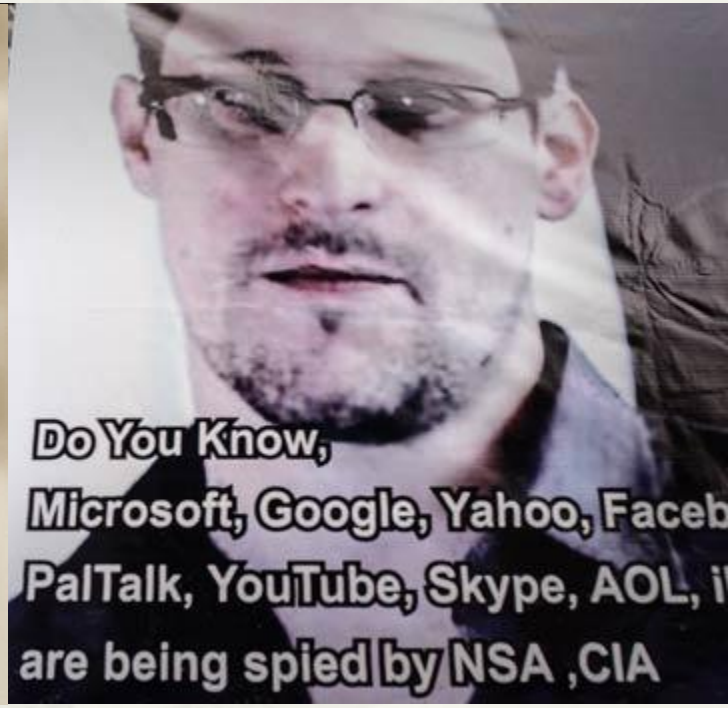
Introduction

Is communication secure?

http://physicsworld.com/cws/article/news/2013/apr/16/alice-and-bob-communicate-without-transferring-a-single-photon,http://www.viasat.com/information-assurance/network-security-appliances

Introduction

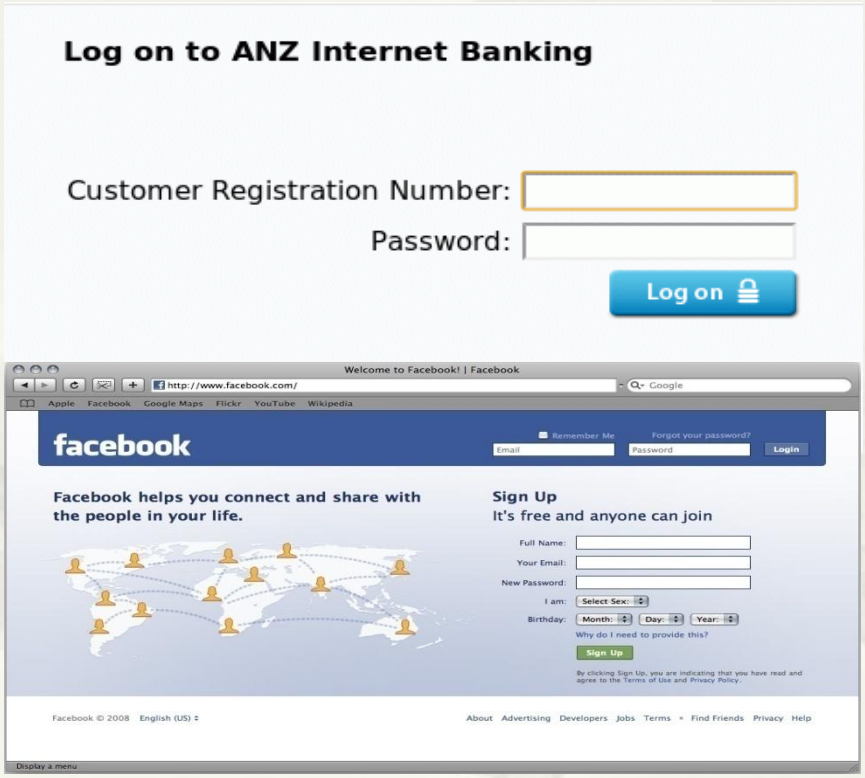
Power of eavesdroppers



http://blog.zap2it.com/pop2it/2013/06/nsa-leaker-edward-snowden-seeks-asylum-in-ecuador-lands-in-moscow-for-the-time-being.html
http://rt.com/usa/obama-internet-wiretap-surveillance-009/

Introduction

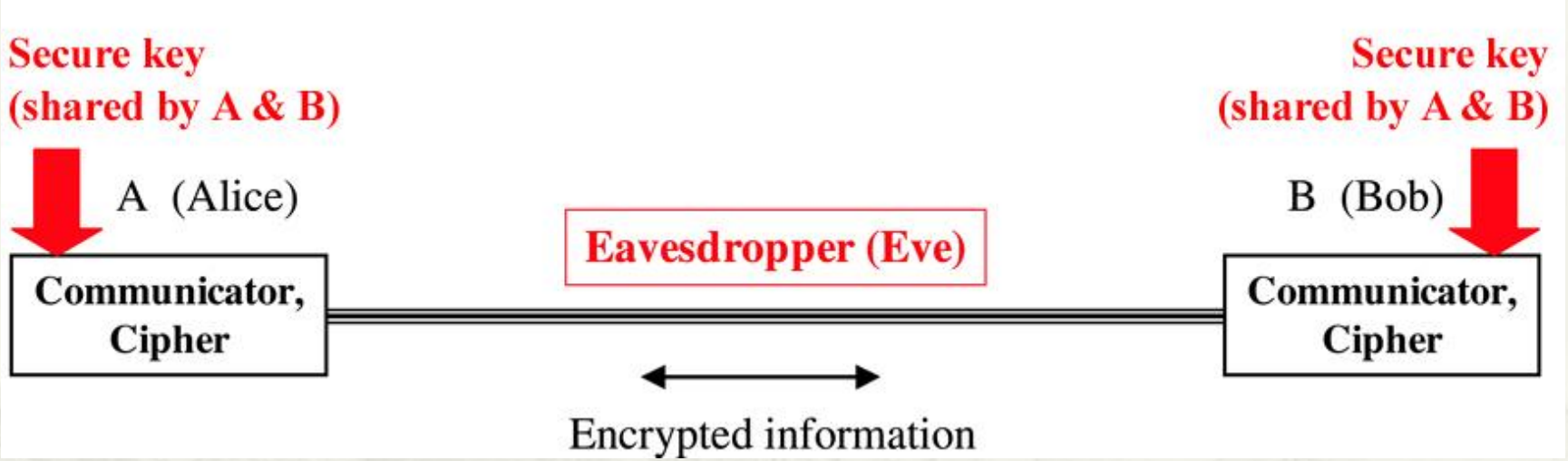
Importance of cryptography



http://www.lemis.com/grog/photos/Photos.php?dirdate=20131025,http://www.flickr.com/photos/psylum/2982646566/,http://alexansary.tv/george-soros-bet-1-3-billion-stock-market-will-fall/

Encryption

One time pad – share the key



Source: http://spie.org/x16669.xml

- The first unbreakable cipher [1]

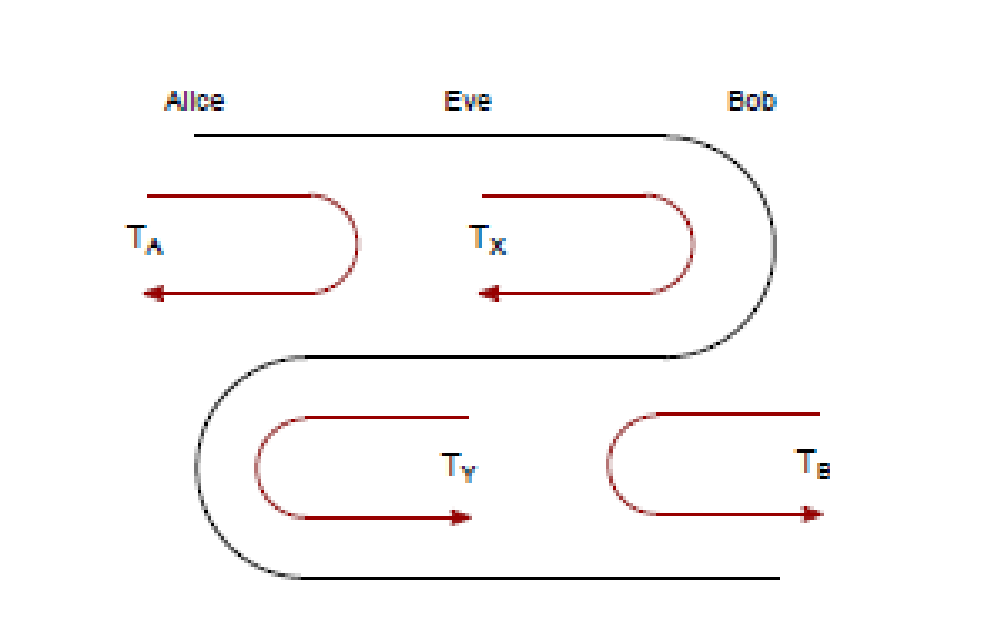
Encryption

Round trip times

Common transit time in theory

Noise disturbing

Different transit time for eavesdropper



Source: L. Gunn, J. Chappell, A. Allison & D. Abbott

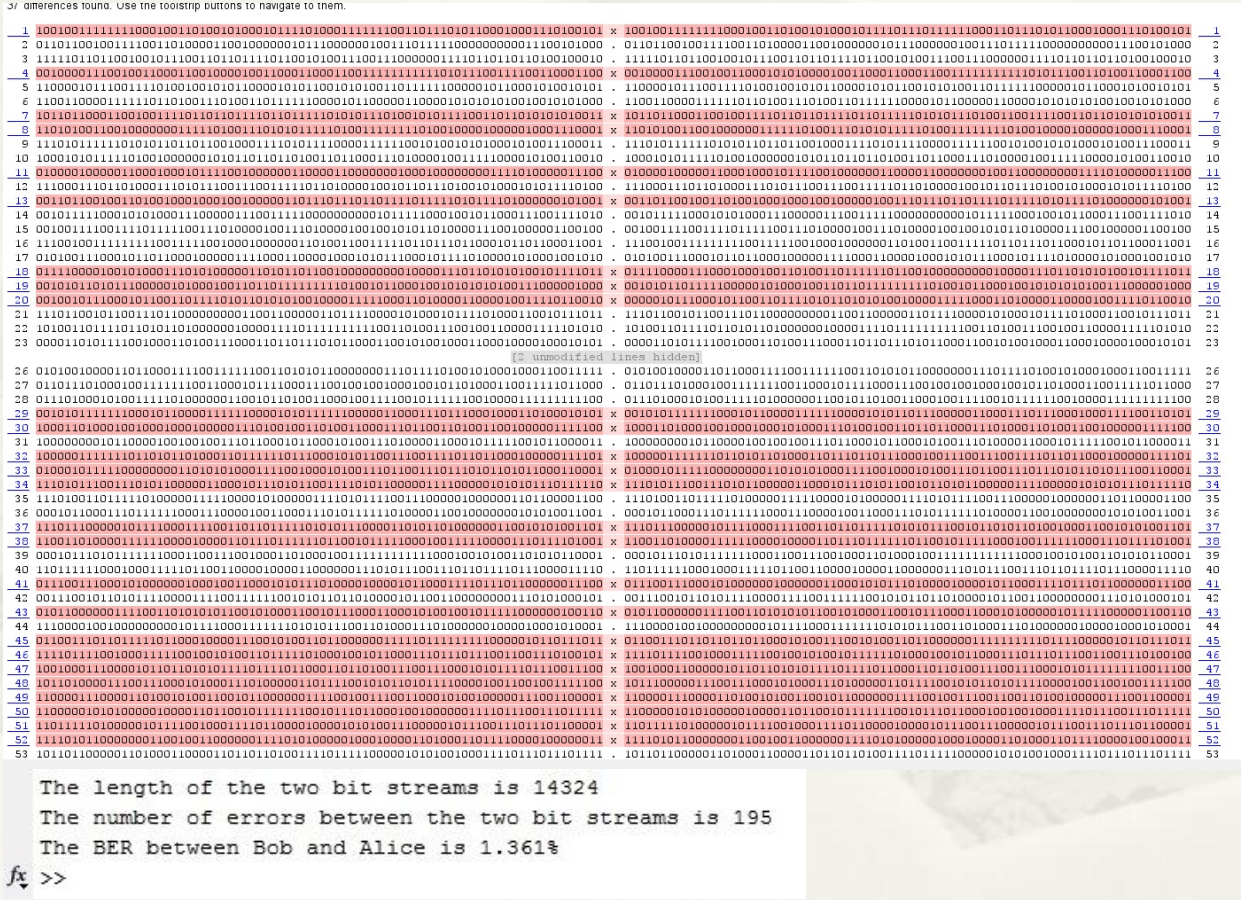
Timing based encryption

Steady channel

Source:
https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Timing_Based_Encryption:_Test_Case_5

Timing based encryption

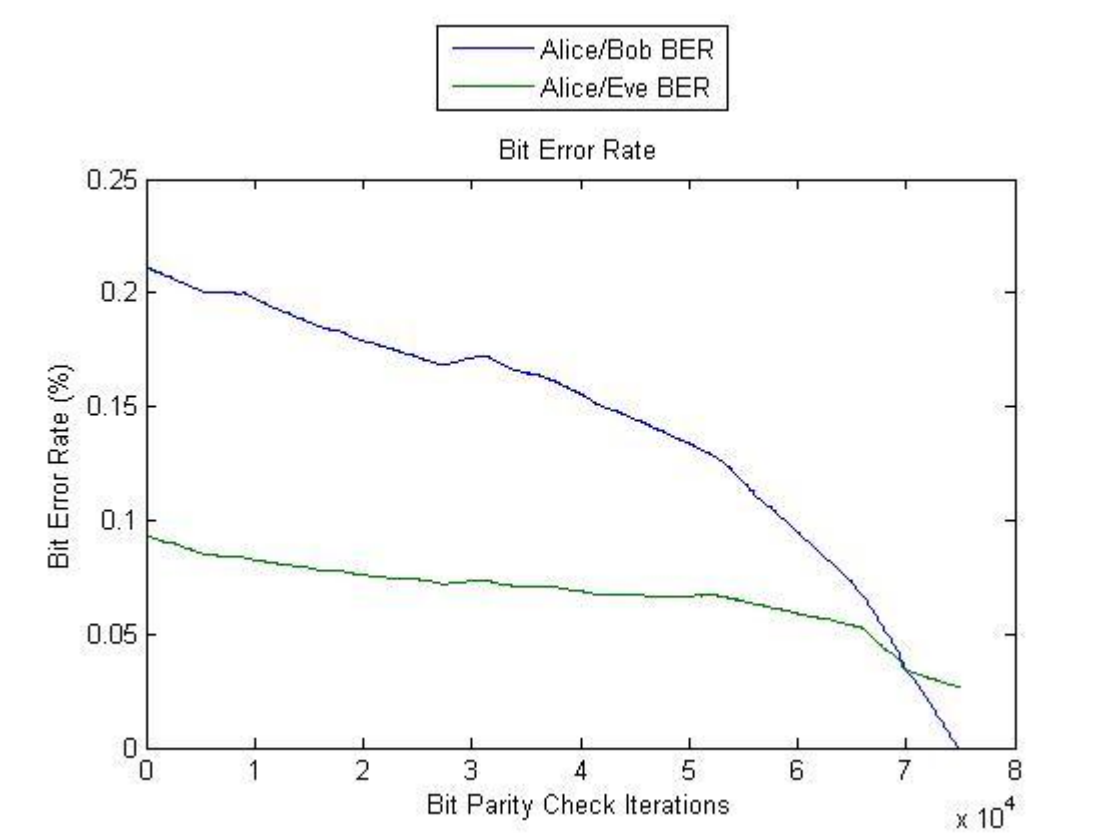
Noise channel



Source:
https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Timing_Based_Encryption:_Test_Case_5

Timing based encryption

- Higher BER for Alice/Bob
- Long time in iterations
- Similar percentage in BER for Alice/Bob and Alice/Eve



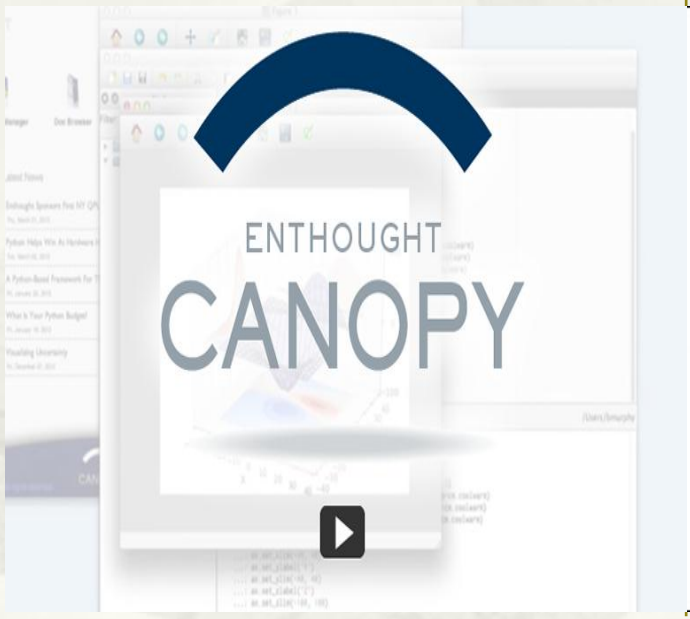
Source: https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve_Output.jpg

Our aims

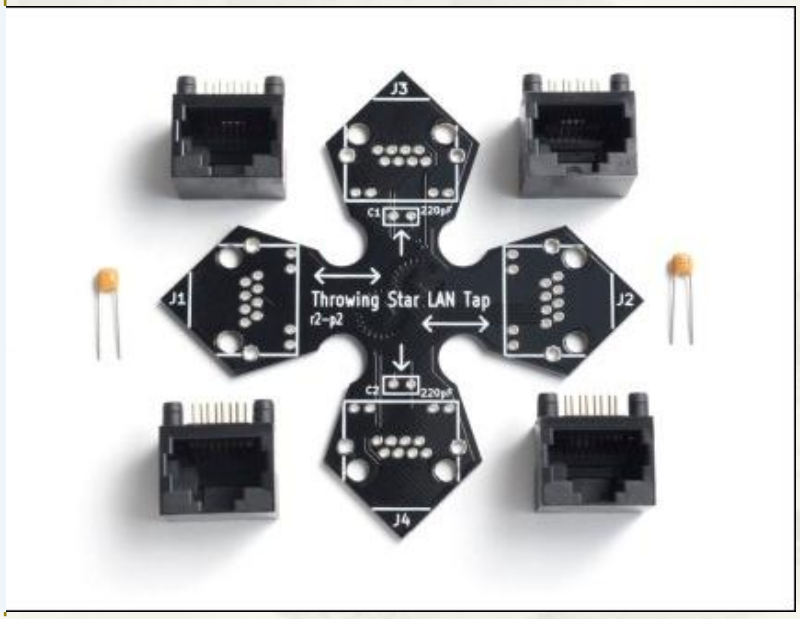
* The efficiency
* The reliability
* The speed
* The utilisation

Approaches

Software	Hardware
Own Personal Computer	Great Scott Gadgets



Source:
https://www.enthought.com/products/canopy/



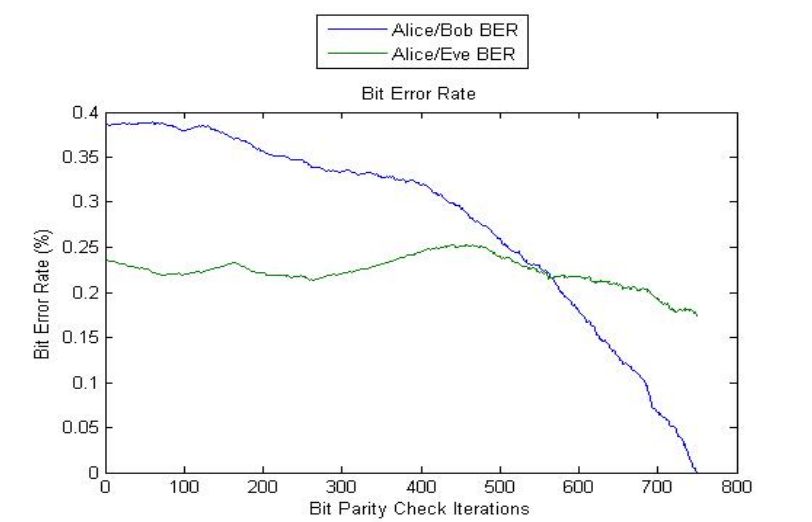
Source:
https://greatscottgadgets.com/throwingstar/

Approaches

Software improvements of encryption

```
     Channel BER confidence interval: (1.20e-01,3.52e-01)
Information reconciliation iterations: 4
 Block size for privacy amplification: 4
     Channel BER confidence interval: (1.03e-01,2.30e-01)
Information reconciliation iterations: 3
 Block size for privacy amplification: 4
11111011010001000011110110111000000011001001010110101010001101001011110100100111
11111011101011010011000001011000001110110100000111100000010111010101000010010111
01000011111111101001011110100100000001011
```

Source: https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Program_output.png

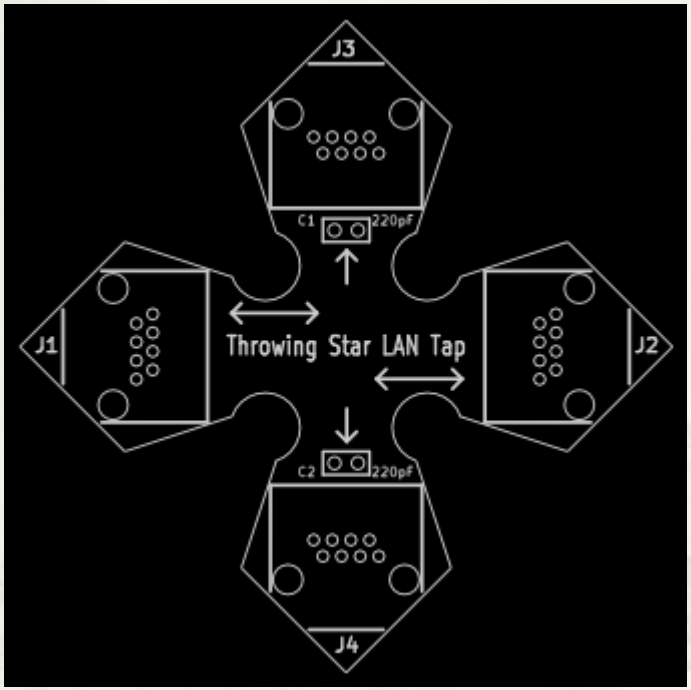


Source: https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve_Output_Test21.jpg

Approaches

Network Tap (eavesdropper)

- J1, J2 – target network to be monitored
- J3, J4 – monitoring ports
- C1,C2 – forcing target network can be monitored



Source: https://greatscottgadgets.com/throwingstar/

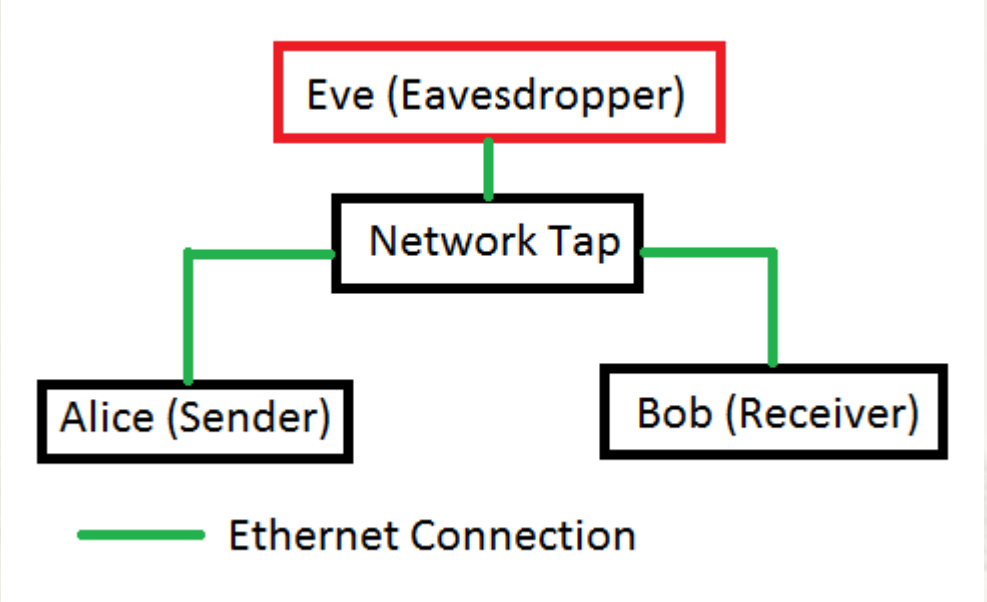
[2] Throwing Star LAN Tap, https://greatscottgadgets.com/throwingstar

Approaches

Sender/Receiver

- Sender – Beagle board / PC
- Receiver – Beagle board / PC
- Eavesdropper – Beagle board

Source:
http://beagleboard.org/Products/BeagleBone

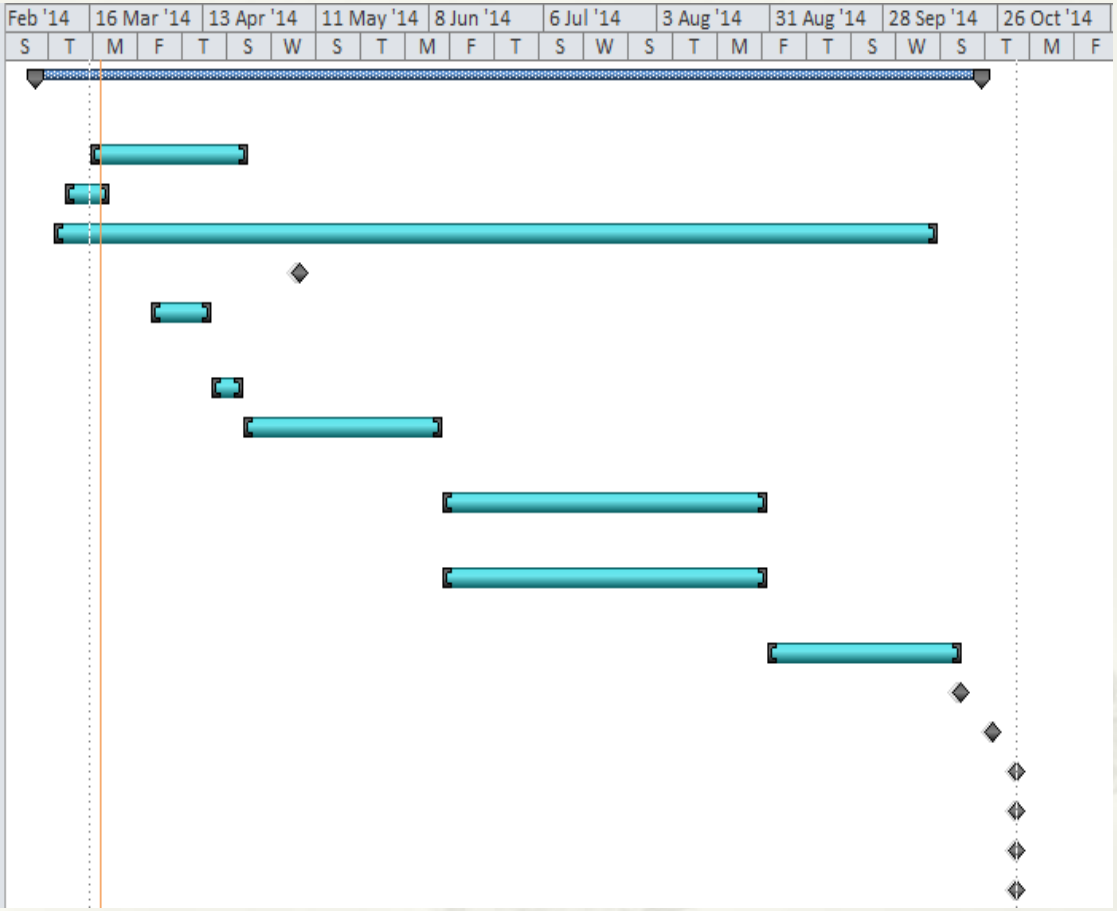


Risk management

Risks	Posibility	Severity	Approaches
Unavailability of team member	Low	High	• Each member sign their own works but with help with each other • Sharing the phone number and email
SVN Blackout	Low	Low	• Sharing the document in Google Drive, file exchange or wiki to make sure each member and supervisors can share the working copies
Lack of technical knowledge	High	High	• Keep talking with each other and supervisors to make sure we understand the technical aspects • Finding useful information in youtube
Physical parts do not arrive and/or do not work in time for project completion	High	Medium	• Ensure constant communication is sought with the suppliers regarding the progress of the delivery • Expedite work on improvements to Timing Based Encryption
Falling behind the schedule	medium	medium	• Re-evaluate the expectations • Talking with supervisors to for extra times
No final solution	Very high	Very low	• Ensure all progress have been completely documented

Time management

Task Name	Duratic	Start	Finish
Is secure communication possible?	167 days	Mon 3/03/14	Tue 21/10/14
documentation	29 days	Sun 16/03/14	Wed 23/04/14
proposal seminar	9 days	Mon 10/03/14	Thu 20/03/14
weekly report	156 days	Fri 7/03/14	Fri 10/10/14
progress report	1 day	Tue 6/05/14	Tue 6/05/14
understanding the example code	11 days	Mon 31/03/14	Mon 14/04/14
network construction	6 days	Tue 15/04/14	Tue 22/04/14
decrease BER in the first transmition (Alice/Bob)	35 days	Wed 23/04/14	Tue 10/06/14
decrease BER after blocking the information	58 days	Wed 11/06/14	Fri 29/08/14
increasing BER for Eve after the blocking	58 days	Wed 11/06/14	Fri 29/08/14
reducing interation times	35 days	Sat 30/08/14	Thu 16/10/14
final seminar	1 day	Thu 16/10/14	Thu 16/10/14
final report	1 day	Fri 24/10/14	Fri 24/10/14
poster	1 day	Thu 30/10/14	Thu 30/10/14
project exhibition	1 day	Thu 30/10/14	Thu 30/10/14
Labelled CD or USB stick	1 day	Thu 30/10/14	Thu 30/10/14
YouTube video	1 day	Thu 30/10/14	Thu 30/10/14



Question and references

[1] L. Gunn, J. Chappell, A. Allison & D. Abbott, ‘Physical-layer encryption on the public internet: a stochastic approach to the Kish-Sethuraman cipher’(June 2013)

[2] Throwing Star LAN Tap, https://greatscottgadgets.com/throwingstar/

[3] Derek Abbott’s Wiki Project, ‘Secure communications without key exchange’, https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Main_Page