Live Session 04

Randomness and Public Key Cryptography

CS 7349

Spring 2024

World Changers Shaped Here

SMU®

Contents

- Security News of the Week
- House Keeping
- Class Presentation – Special Topic
- Concepts: Randomness, PRNGs and Stream Ciphers
- PRFs and Public Key Cryptography

Sources: YouTube/Dr. Dan Boneh, Cryptography 1; www.simonsingh.net; Cryptography and Network Security, William Stallings; schneier.com

House Keeping

- Status of Teams for Term Paper? Topic?
- Term Paper Topic, team, due by 01/28/2024; Checkpoint on 01/29, 01/31
- Submit Quiz 1 and start on Quiz 2
- Quiz 1, 1 week; Homework 1, 2 weeks
- RED ALERT on Research Paper! Teams & Topic NOW!!

Time is of the Essence

Sources: Midjourney via Meta AI

Security News of the Week – Spring 2024

- https://www.wsj.com/tech/cybersecurity/microsoft-reports-hack-by-nation-state-actor-0ffd57ca?mod=cybersecurity_news_article_pos2
  - A nation-state actor breached the emails of MSFT/HPE senior leadership
- https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/
  - ~7M users breached, more and longer than previously thought
- https://www.cio.com/article/1298075/a-new-era-of-cybersecurity-with-ai-predictions-for-2024.html
  - Sponsored report detailing the rise of AI in cyberattacks and mitigation

Source: wsj.com; techcrunch.com;cio.com

New Urban Dictionary terms

- SIM swapping

- Maryland woman loses $17K in SIM card swap scam despite two-factor authentication | I-Team | WJLA
  - 17k drained from BoA account after Verizon SIM swap

CS 7349 – Tying it all together

- INTRODUCTION TO CS7349 AND THE THREAT LANDSCAPE
- INTRODUCTION TO NETWORKS
- SYMMETRIC KEY CRYPTO
- USING SYMMETRIC KEY CIPHERS
- RANDOMNESS AND PSEUDORANDOM NUMBERS
- PUBLIC KEY CRYPTO/Team Paper

Confidentiality

- HASH FUNCTIONS
- MESSAGE AUTHENTICATION CODES
- KEY MANAGEMENT
- IDENTITY AND ACCESS MANAGEMENT

Integrity Availability

- NETWORK SECURITY
- SECURITY – CLOUD, WIRELESS/5G, DDoS, SASE, IoT, SDN, Smart Cities
- FRAMEWORKS, STANDARDS, OPERATIONS, Governance/Risk/Compliance
- REVIEW/ADDITIONAL TOPICS

Networks/Application

Spring schedule

Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

Class Presentation - Special Topic

- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - ~~Adu, Aliliele~~, Braden, Cho, Dominguez, Garcia, Garza, Gibbs, Guo, Hennes, Jackson, Kharwadhkar, Kucera, Lei, Liang, Lim, Lin, Liu, Magee, Mandalaneni, Mathew, Miller, Nagamanickam, DPatel, PPatel, Pittman, Sanaboyina, Singh, Skochdopole, Swigart, Taghavi, Wang, Werth, Zhai

Project Timeline (For 9 page paper)

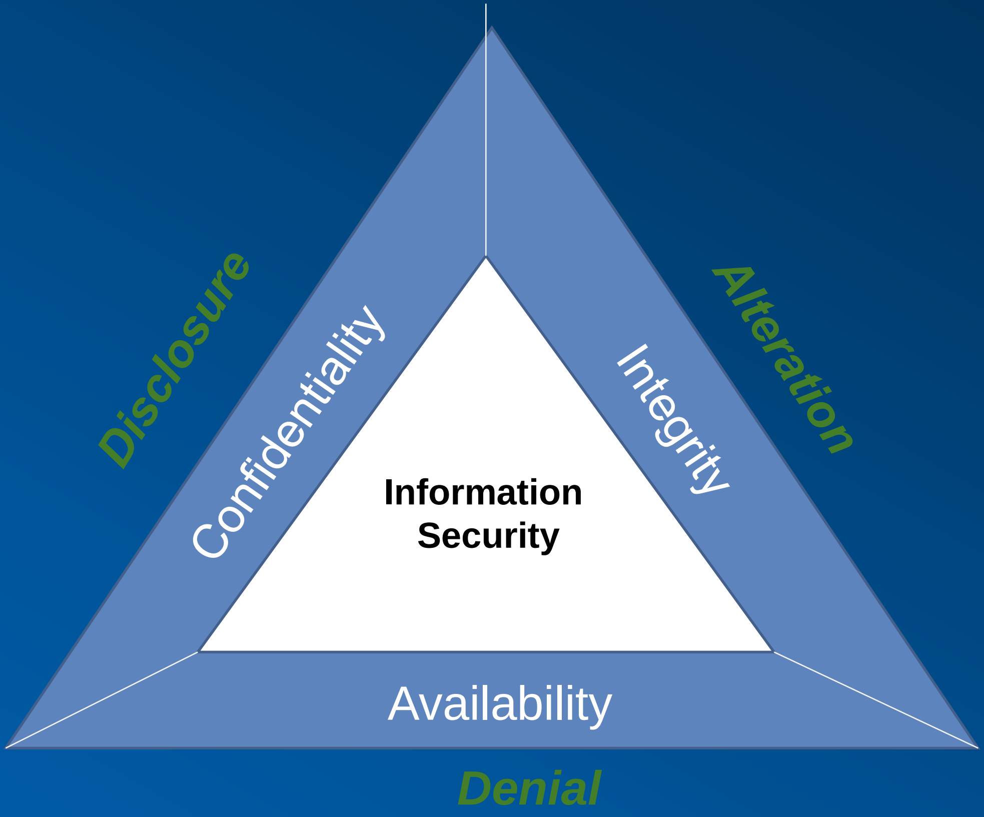
- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

A LaTex template and example paper will be provided

Project – 1st deliverable

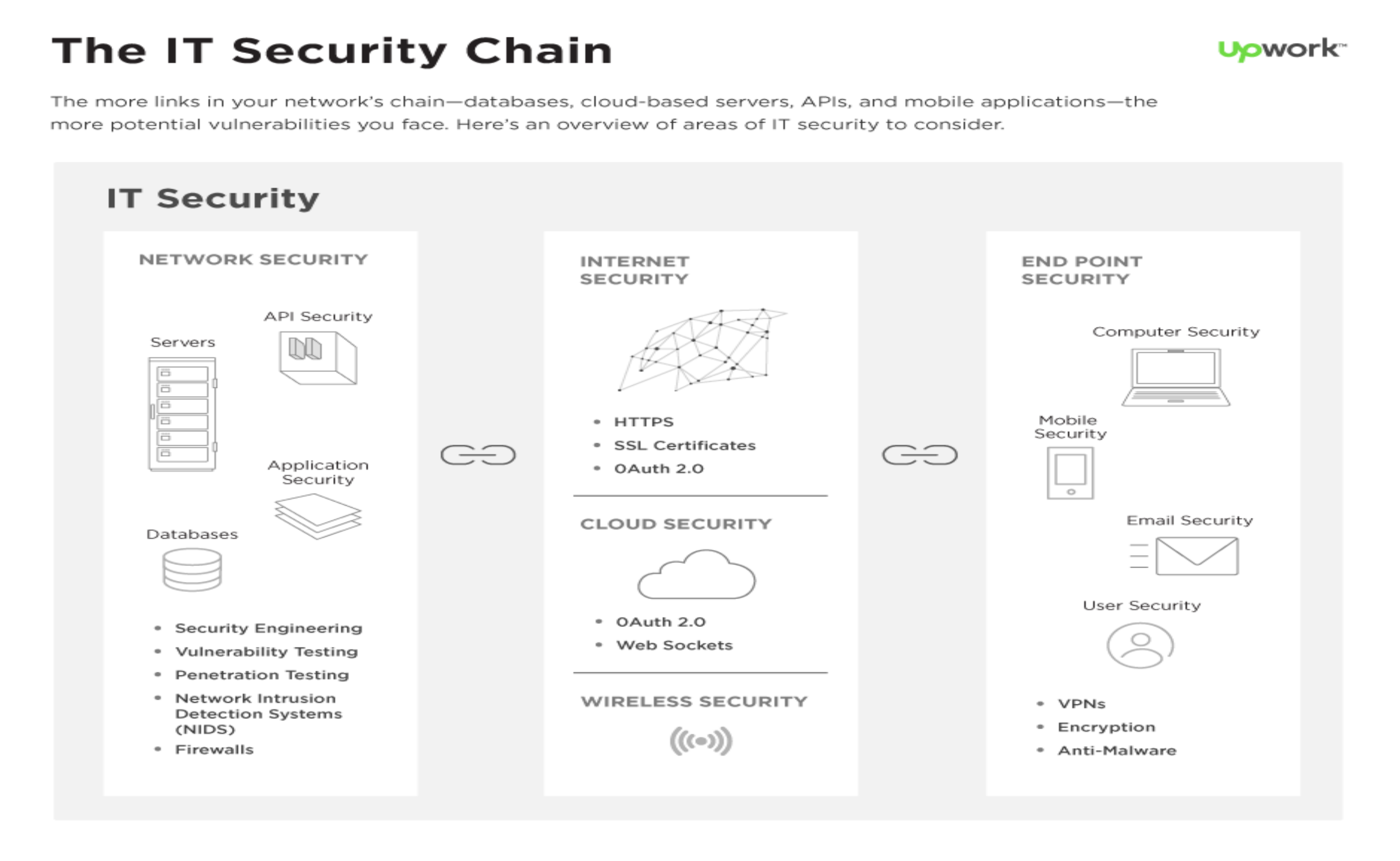
- Team projects (3 per team)
- Choose topic (from topic list or your own)*
- Within topic, identify problem to be addressed (no survey projects, only problem solving projects - survey is a part of your problem solution and is contained in the final paper)
- Confirm problem with professor

InfoSec, CIA, Threats



Source: “Information Security Illuminated”, Solomon and Chapple, 2005, Sudbury, MA:Jones and Bartlett.

Network Security Basics



The IT Security Chain

The more links in your network's chain—databases, cloud-based servers, APIs, and mobile applications—the more potential vulnerabilities you face. Here's an overview of areas of IT security to consider.

IT Security

NETWORK SECURITY

- Security Engineering
- Vulnerability Testing
- Penetration Testing
- Network Intrusion Detection Systems (NIDS)
- Firewalls

INTERNET SECURITY

- HTTPS
- SSL Certificates
- OAuth 2.0

CLOUD SECURITY

- OAuth 2.0
- Web Sockets

WIRELESS SECURITY

END POINT SECURITY

- VPNs
- Encryption
- Anti-Malware

Source: Upwork Global, Inc

Randomness & Pseudorandom Numbers

CS 7349

Spring 2024

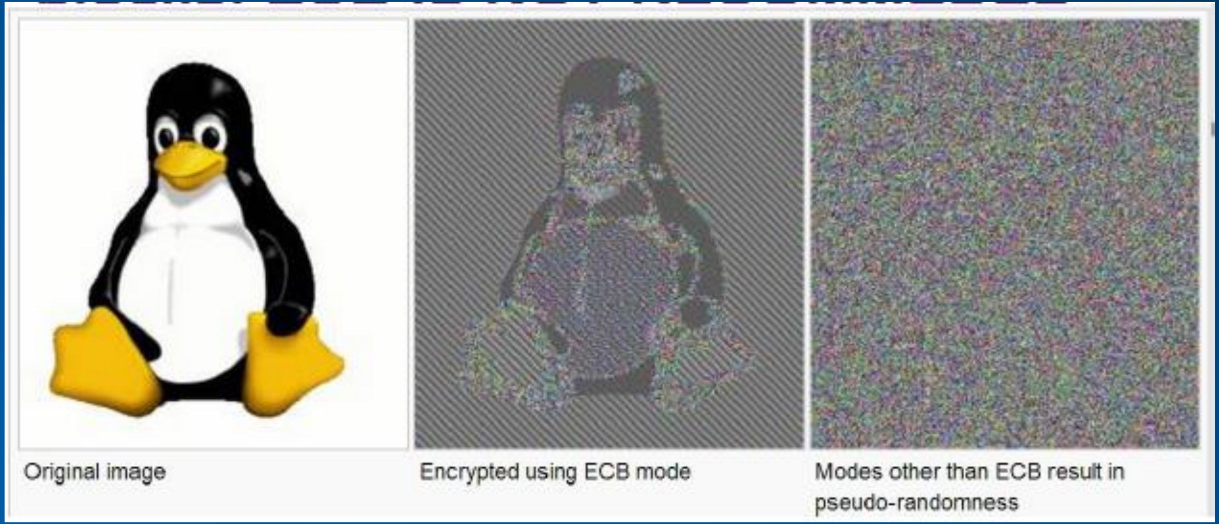
World Changers
Shaped Here

SMU®

Randomness

- Burning questions?
- Why randomness? Why so important?
  - Confusion and Diffusion
- Randomness: Uniform, Independent, Unpredictable
- PRNG: Efficient, Deterministic, Periodic
  - Cryptographically secure PRNG, PRFs (Hash Functions)
- TRNG: Not efficient, non-deterministic, non-periodic

Modes of Operation – remember?



Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

PRNG

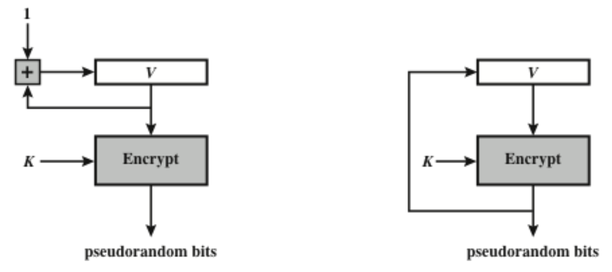
Purpose-built Algorithms

- Linear Congruential Generator:
  - $X_{n+1}=(aX_n+c) \bmod m$
- BBS Generator: CSPRBG, purpose-built
- PRGA for RC4 stream cipher

Based on existing crypto algorithms

- Symmetric Block Ciphers: OFB, CTR (NIST, ANSI, IETF)
- Asymmetric Ciphers: factoring a prime*
- Hash Functions/Message Authentication Codes: PRFs

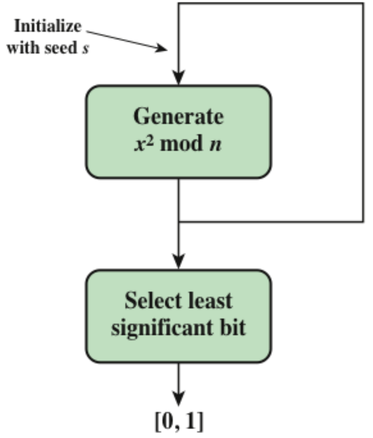
PRNG



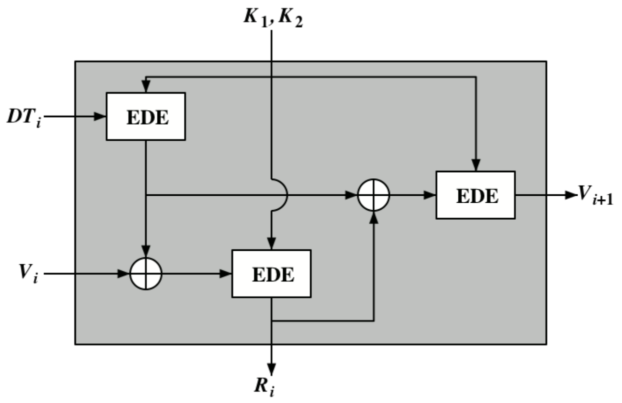
(a) CTR Mode

(b) OFB Mode

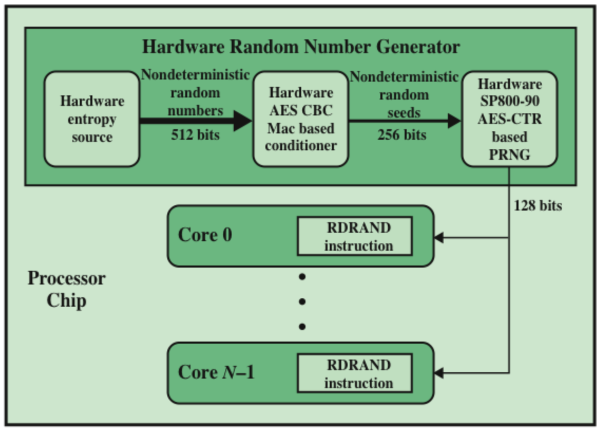
PRNG Mechanisms Based on Block Ciphers



Blum Blum Shub Block Diagram



ANSI X9.17 Pseudorandom Number Generator


Hardware Random Number Generator
Hardware entropy source
Nondeterministic random numbers
512 bits
Hardware AES CBC Mac based conditioner
Nondeterministic random seeds
256 bits
Hardware SP800-90 AES-CTR based PRNG
128 bits
Core 0
RDRAND instruction
Processor Chip
Core N–1
RDRAND instruction

Intel Processor Chip with Random Number Generator

Game Time! – Generate Random Numbers

Generate a sequence of 100 bits and write down the results. Judges will decide which sequence is random.

- Group 1 = Judges
- Group 2 = Human bit generator (members will generate 0, 1 from their mind)
- Group 3 = Coin Flips generate bits (heads 0, Tails 1)
- Post your results on the wall
- Judges to decide which sequence is random.

RC4 Stream Cipher

https://www.coursera.org/learn/crypto/lecture/mQAkP/real-world-stream-ciphers

1. Initialize an array of 256 bytes.
2. Run the Key Scheduling Algorithm (KSA)
3. Run the PRGA on the KSA output to generate Key stream.
4. XOR data with key stream

Initialize

```
for i = 0 to 255
   do
   S[i] = i;
   T[i] = K[i mod keylen];
```

KSA

```
j = 0;
for i = 0 to 255
   do
      j = (j + S[i] + T[i]) mod
   256;
      Swap (S[i], S[j]);
```

PRGA

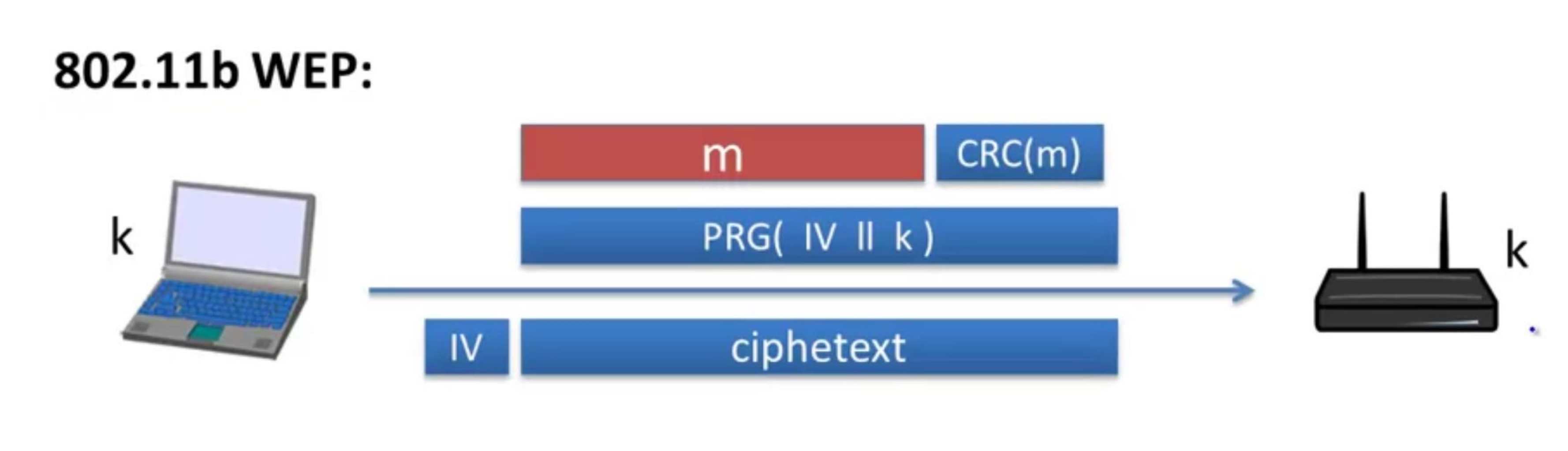
```
 i, j = 0;
for (int x = 0; x < byteLen; x++)

   do
   i = (i + 1) mod 256;
   j = (j + S[i]) mod 256;
   Swap (S[i], S[j]);
   t = (S[i] + S[j]) mod 256;
   k = S[t];
```

Security Design Errors

- Weakness in Microsoft PPTP and in WEP by Boneh
- https://www.coursera.org/learn/crypto/lecture/euFJx/attacks-on-stream-ciphers-and-the-one-time-pad (starting at 4:29-13:35)
- Paper on WEP Attacks
  - **http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf**

802.11b WEP



802.11b WEP:

WEP Vulnerability Summary

1. Industry-driven committee, open standard with no public review.
2. Access point to mobile stations: same symmetric key (like a password for the whole company)
3. Integrity check with CRC. Erroneous bits are detected. Deliberate errors not detected. PACKET MODIFICATION
4. No state information. So REPLAY attacks can be launched. Modified packets can be replayed.
5. 24-bit IV concatenated with 104-bit key.IV initialized with 0 (predictable, not random). 24-bit IV has collisions after 2^24 packets. Lack of randomness. Small key size. Susceptible to MITM
6. RC4 was prohibited for use in ALL versions of TLS by RFC7465 (https://www.rfc-editor.org/info/rfc7465)

Public Key Cryptography

CS 7349

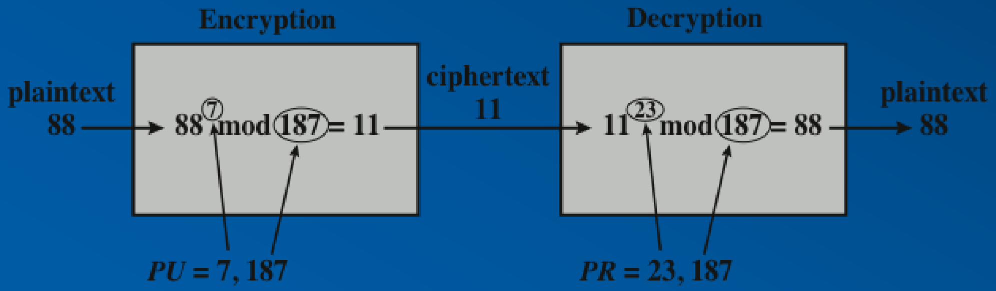
Spring 2024

World Changers Shaped Here

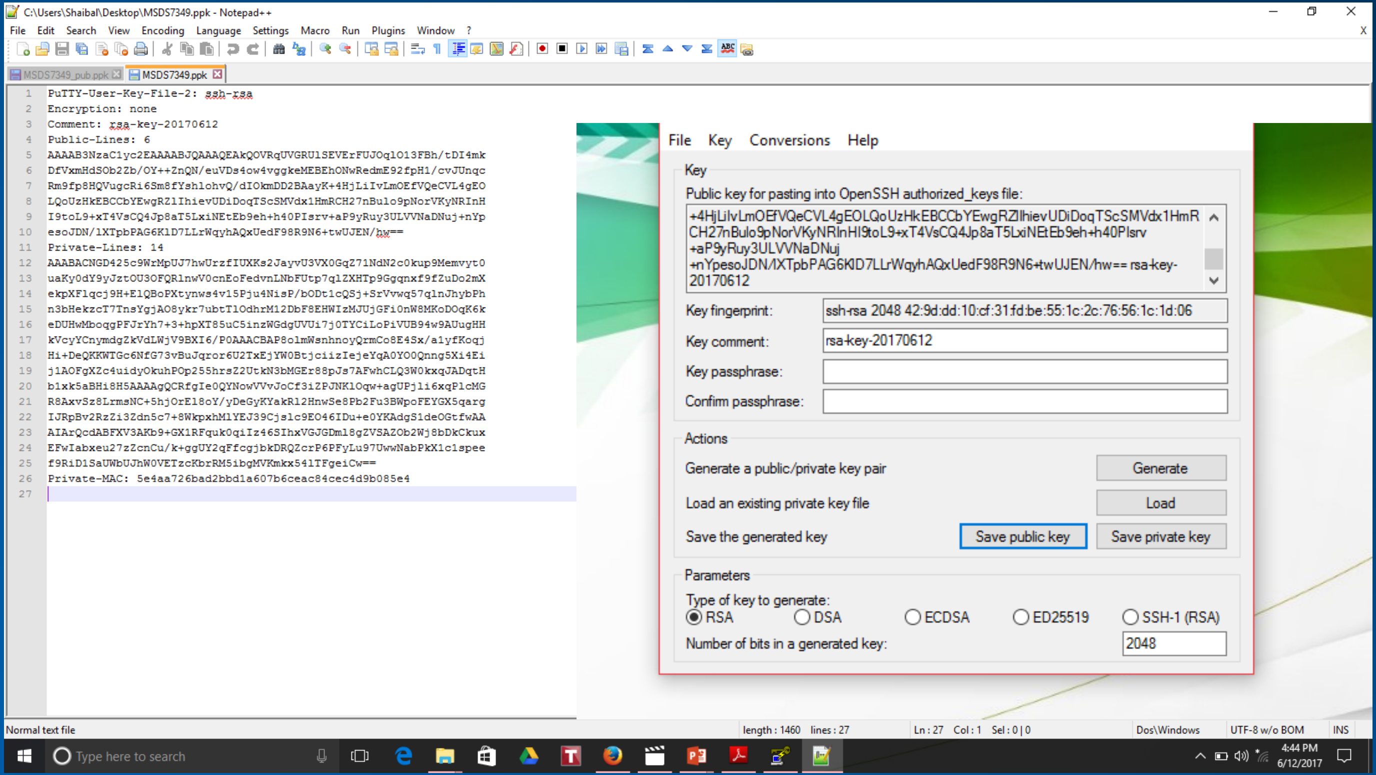
SMU®

Public Key Crypto

- Burning questions?
- The math behind PKC?
  - https://www.youtube.com/watch?v=oR0_LPbWxe4 (start, 3:19)
  - http://simonsingh.net/media/online-videos/cryptography/the-science-of-secrecy-going-public/
  - Concepts (integers, exponent, 1024/2048-bit keys)



Public private keypair – PuttyGen


C:\Users\Shaibal\Desktop\MSDS7349.ppk - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
MSDS7349_pub.ppk
MSDS7349.ppk
File Key Conversions Help
Generate
Load
Save public key
Save private key
Normal text file
length : 1460 lines : 27
Ln : 27 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8 w/o BOM
INS
Type here to search
4:44 PM
6/12/2017

```
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20170612
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEAkQOVRqUVGRUlSEVErFUJOqlO13FBh/tDI4mk
DfVxmHdSOb2Zb/OY++ZnQN/euVDs4ow4vggkeMEBEhONwRedmE92fpH1/cvJUnqc
Rm9fp8HQVugcRi6Sm8fYshlohvQ/dIOkmDD2BAayK+4HjLiIvLmOEfVQeCVL4gEO
LQoUzHkEBCCbYEwgRZlIhievUDiDoqTScSMVdx1HmRCH27nBulo9pNorVKyNRInH
I9toL9+xT4VsCQ4Jp8aT5LxiNEtEb9eh+h40PIsrv+aP9yRuy3ULVVNaDNuj+nYp
esoJDN/lXTpbPAG6KlD7LLrWqyhAQxUedF98R9N6+twUJEN/hw==
Private-Lines: 14
AAABACNGD425c9WrMpUJ7hwUrzfIUXKs2JayvU3VX0GqZ71NdN2c0kup9Memvyt0
uaKy0dY9yJztOU3OFQRlnwV0cnEoFedvnLNbFUtp7qlZXHTp9Ggqnxf9fZuDo2mX
ekpXFlqcj9H+ElQBoPXtynws4v15Pju4NisP/bODt1cQSj+SrVvwq57qlnJhybPh
n3bHekzcT7TnsYgjAO8ykr7ubtTlOdhrM12DbF8EHWIzMJUjGFi0nW8MKoDOqK6k
eDUHwMboqgPFJrYh7+3+hpXT85uC5inzWGdgUVUi7j0TYCiLoPiVUB94w9AUugHH
kVcyYCnymdgZkVdLWjV9BXI6/P0AAACBAP8olmWsnhnoyQrmCo8E4Sx/a1yfKoqj
Hi+DeQKKWTGc6NfG73vBuJqror6U2TxEjYW0BtjciizIejeYqA0YO0Qnng5Xi4Ei
j1AOFgXZc4uidyOkuhPOp255hrsZ2UtkN3bMGEr88pJs7AFwhCLQ3W0kxqJADqtH
b1xk5aBHi8H5AAAAgQCRfgIe0QYNowVVvJoCf3iZPJNKlOqw+agUPjli6xqPlcMG
R8AxvSz8LrmsNC+5hjOrEl8oY/yDeGyKYakRl2HnwSe8Pb2Fu3BWpoFEYGX5qarg
IJRpBv2RzZi3Zdn5c7+8WkpxhMlYEJ39Cjslc9EO46IDu+e0YKAdgS1deOGtfwAA
AIArQcdABFXV3AKb9+GX1RFquk0qiIz46SIhxVGJGDml8gZVSAZOb2Wj8bDkCkux
EFwIabxeu27zZcnCu/k+ggUY2qFfcgjbkDRQZcrP6PFyLu97UwwNabPkX1c1spee
f9RiD1SaUWbUJhW0VETzcKbrRM5ibgMVKmkx54lTFgeiCw==
Private-MAC: 5e4aa726bad2bbd1a607b6ceac84cec4d9b085e4
```

Key

Public key for pasting into OpenSSH authorized_keys file:

```
+4HjLiIvLmOEfVQeCVL4gEOLQoUzHkEBCCbYEwgRZlIhievUDiDoqTScSMVdx1HmR
CH27nBulo9pNorVKyNRInHI9toL9+xT4VsCQ4Jp8aT5LxiNEtEb9eh+h40PIsrv
+aP9yRuy3ULVVNaDNuj
+nYpesoJDN/lXTpbPAG6KlD7LLrWqyhAQxUedF98R9N6+twUJEN/hw== rsa-key-
20170612
```

Key fingerprint: ssh-rsa 2048 42:9d:dd:10:cf:31:fd:be:55:1c:2c:76:56:1c:1d:06

Key comment: rsa-key-20170612

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

RSA

- RSA makes use of an expression with exponentials
- Plaintext is encrypted in blocks with each block having a binary value less than some number *n*
- Encryption and decryption are of the following form, for some plaintext block *M* and ciphertext block C

$$C = M^e \bmod n$$

$$M = C^d \mathit{mod}\ n = (M^e)^d \mathit{mod}\ n = M^{ed} \mathit{mod}\ n$$

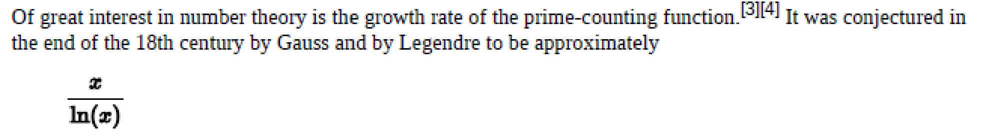
- Both sender and receiver must know the value of *n*
- The sender knows the value of *e*, and only the receiver knows the value of *d*
- This is a public-key encryption algorithm with a public key of *PU={e,n}* and a private key of *PR={d,n}*
- *https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html*

Public Key Crypto/RSA Vulnerabilities

- Vulnerabilities
  - Somebody’s generating large primes and making a table
  - Brute force attack (use larger keys. Reduces usability. Key Exchange and signature applications)
  - Probable message attack
    - Mitigate: pad with extra bits Optimal Asymmetric Encryption Padding
  - Unproven if private key can be derived from public key
    - Trapdoor One Way Function reversal
- RSA: Brute force, timing and DPA, Factoring, hardware and CCA (chosen ciphertext attack)

Public Key Crypto

- Question asked in class: How do we know if there are collisions?
- Answer: You DON’T
- Math:



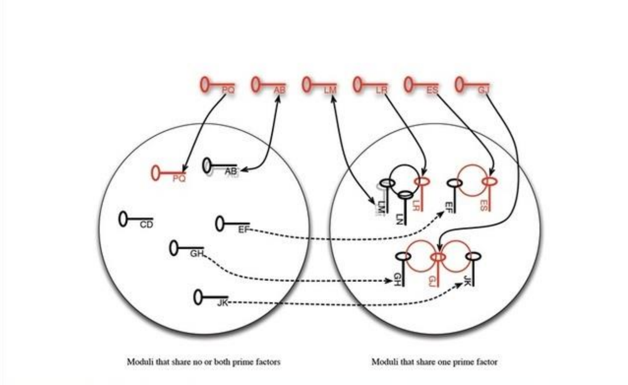
Of great interest in number theory is the growth rate of the prime-counting function.[3][4] It was conjectured in the end of the 18th century by Gauss and by Legendre to be approximately

$$\frac{x}{\ln(x)}$$

- Source: Wikipedia, https://eprint.iacr.org/2012/064.pdf
  - 12720 of 4.7 million distinct 1024-bit RSA moduli had a single large prime factor in common
  - 26965 of 11.4 million RSA moduli are vulnerable, including ten 2048-bit ones

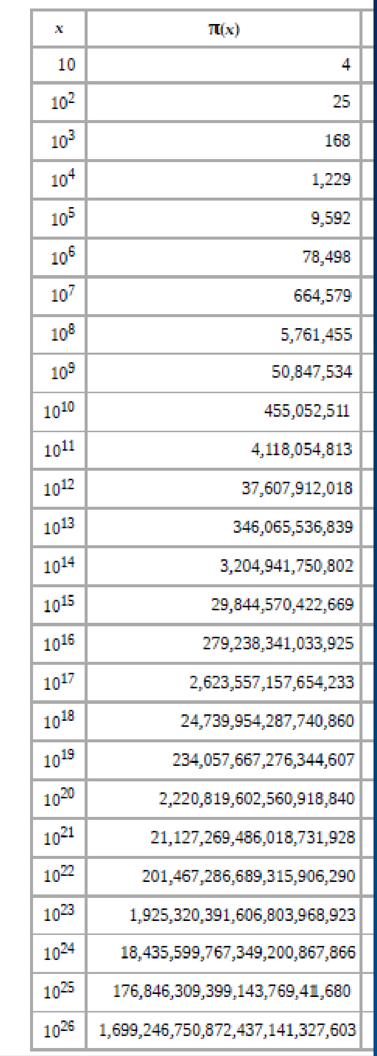
Public Key Crypto

- 1024 bits ~ $2^{1024} = 1.8^{308}$
- 2048 bits ~ $2^{2048} = 3.2^{616}$
- Chances of collision for random picks?
  - 1 or 2 prime numbers to factor N
  - 4 out of every 1,000 public keys protecting webmail, online banking, and other sensitive online services provide no cryptographic security



Moduli that share no or both prime factors

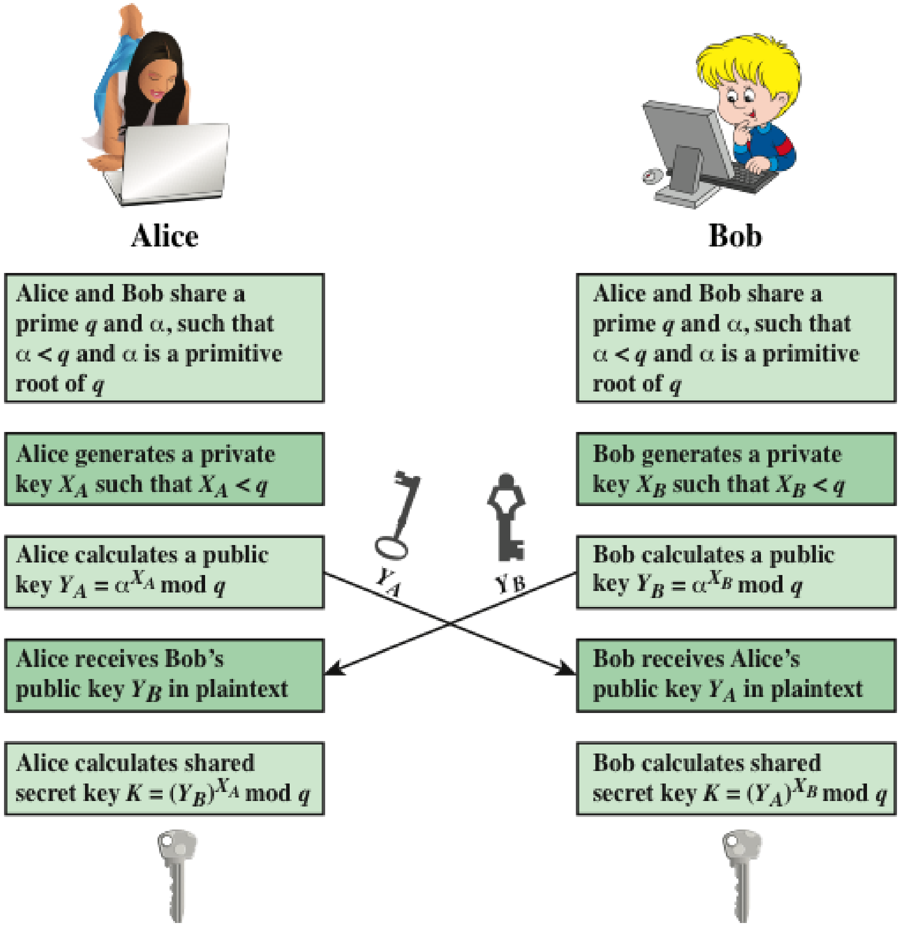
Moduli that share one prime factor



x	π(x)
10	4
10^{2}	25
10^{3}	168
10^{4}	1,229
10^{5}	9,592
10^{6}	78,498
10^{7}	664,579
10^{8}	5,761,455
10^{9}	50,847,534
10^{10}	455,052,511
10^{11}	4,118,054,813
10^{12}	37,607,912,018
10^{13}	346,065,536,839
10^{14}	3,204,941,750,802
10^{15}	29,844,570,422,669
10^{16}	279,238,341,033,925
10^{17}	2,623,557,157,654,233
10^{18}	24,739,954,287,740,860
10^{19}	234,057,667,276,344,607
10^{20}	2,220,819,602,560,918,840
10^{21}	21,127,269,486,018,731,928
10^{22}	201,467,286,689,315,906,290
10^{23}	1,925,320,391,606,803,968,923
10^{24}	18,435,599,767,349,200,867,866
10^{25}	176,846,309,399,143,769,411,680
10^{26}	1,699,246,750,872,437,141,327,603

Diffie-Hellman Key Exchange

- First published public-key algorithm
- A number of commercial products employ this key exchange technique
- Purpose is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages
- The algorithm itself is limited to the exchange of secret values
- Its effectiveness depends on the difficulty of computing discrete logarithms



Alice

Alice and Bob share a prime q and α, such that $\alpha < q$ and α is a primitive root of q

Alice generates a private key X_A such that $X_A < q$

Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$

Alice receives Bob's public key Y_B in plaintext

Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$

Bob

Alice and Bob share a prime q and α, such that $\alpha < q$ and α is a primitive root of q

Bob generates a private key X_B such that $X_B < q$

Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$

Bob receives Alice's public key Y_A in plaintext

Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$

Figure 10.1 Diffie-Hellman Key Exchange

Key Exchange Protocols

- Users could create random private/public Diffie-Hellman keys each time they communicate
- Users could create a known private/public Diffie-Hellman key and publish in a directory, then consulted and used to securely communicate with them
- Vulnerable to Meet-in-the-Middle-Attack
- Authentication of the keys is needed

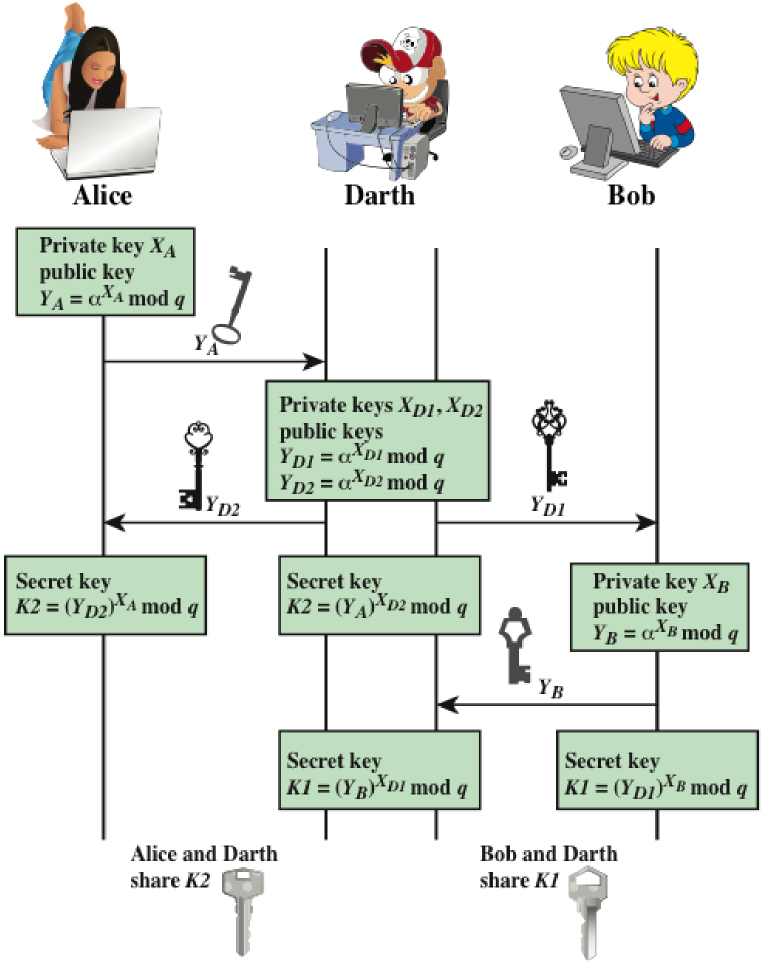

Alice
Darth
Bob
Private key X_A
public key
$Y_A = \alpha^{X_A} \bmod q$
Y_A
Private keys X_{D1}, X_{D2}
public keys
$Y_{D1} = \alpha^{X_{D1}} \bmod q$
$Y_{D2} = \alpha^{X_{D2}} \bmod q$
Y_{D2}
Y_{D1}
Secret key
$K2 = (Y_{D2})^{X_A} \bmod q$
Secret key
$K2 = (Y_A)^{X_{D2}} \bmod q$
Private key X_B
public key
$Y_B = \alpha^{X_B} \bmod q$
Y_B
Secret key
$K1 = (Y_B)^{X_{D1}} \bmod q$
Secret key
$K1 = (Y_{D1})^{X_B} \bmod q$
Alice and Darth
share $K2$
Bob and Darth
share $K1$

Figure 10.2 Man-in-the-Middle Attack

El-Gamal Public Key Cryptography

- Announced in 1984 by T. Elgamal
- Public-key scheme based on discrete logarithms closely related to the Diffie-Hellman technique
- Used in the digital signature standard (DSS) and the S/MIME e-mail standard
- Global elements are a prime number q and a which is a primitive root of q
- Security is based on the difficulty of computing discrete logarithms

Elliptic Curve Arithmetic

- Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA
  - The key length for secure RSA use has increased over recent years and this has put a heavier processing load on applications using RSA
- Elliptic curve cryptography (ECC) is showing up in standardization efforts including the IEEE P1363 Standard for Public-Key Cryptography
- Principal attraction of ECC is that it appears to offer equal security for a far smaller key size
- Confidence level in ECC is not yet as high as that in RSA

Security of Elliptic Curve Cryptography

- Depends on the difficulty of the elliptic curve logarithm problem
- Fastest known technique is “Pollard rho method”
- **Compared to factoring, can use much smaller key sizes than with RSA**
- For equivalent key lengths computations are roughly equivalent
- Hence, for similar security ECC offers significant computational advantages

Thank You!

World Changers
Shaped Here

SMU®

Project Reports

- **Use the LaTex template** provided for your project paper submissions.
- **Read** the Sample paper and **follow** its directions as appropriate in writing your paper.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents.
- https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)

Project Abstract and Intro

- **Abstract** structure (100 word limit for 6 pages)
  - start with statement of what is presented
  - motivate the problem
  - discuss details of what is done at a high level
  - state the main conclusions
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper
  - state the outline for the rest of the paper
    - Conclusions are not stated in the introduction.

Project Paper

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 9 pages exactly. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/read/brpdfvsxsjww#8886a4 ←Paper template