An Introduction to Cryptography

Part 2: Modern Crypto

Anthony Kosednar

My Background

- Education
  - Number Theory, Field Theory, Cryptography and Statistics while in Highschool @ ASU
  - Studied Aerospace Engineering - Astronautics @ ASU
  - DHS Cybersecurity Training for Industrial Control Systems – SCADA, DCS, PLC, Embedded Control
  - GIAC Exploit Researcher and Advanced Penetration Tester - GXPN
- Part of these groups:
  - InfraGard
  - North American Network Operations Group (NANOG)
  - American Institute of Aeronautics and Astronautics (AIAA)
  - National Society of Professional Engineers (NSPE)
- I work in doing mainly cybersecurity for critical infrastructure
  - In the past consulted for sporting venues and large events (Arizona Cardinals, Arizona Board of Tourism, NFL, Super Bowl XLIX, Fiesta Bowl)
  - Currently work for a large publicly traded company

A Review
Kerckhoff's Principle

- Auguste Kerckhoff, 1883
  - Direct translation
    - "The system must not require secrecy and can be stolen by the enemy without causing trouble"
  - Rephrased
    - "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge"
  - This is in contrast to the common approach of "security through obscurity", where the security depends on people not knowing what the security measures are or how they work

Principles of Modern Cryptography

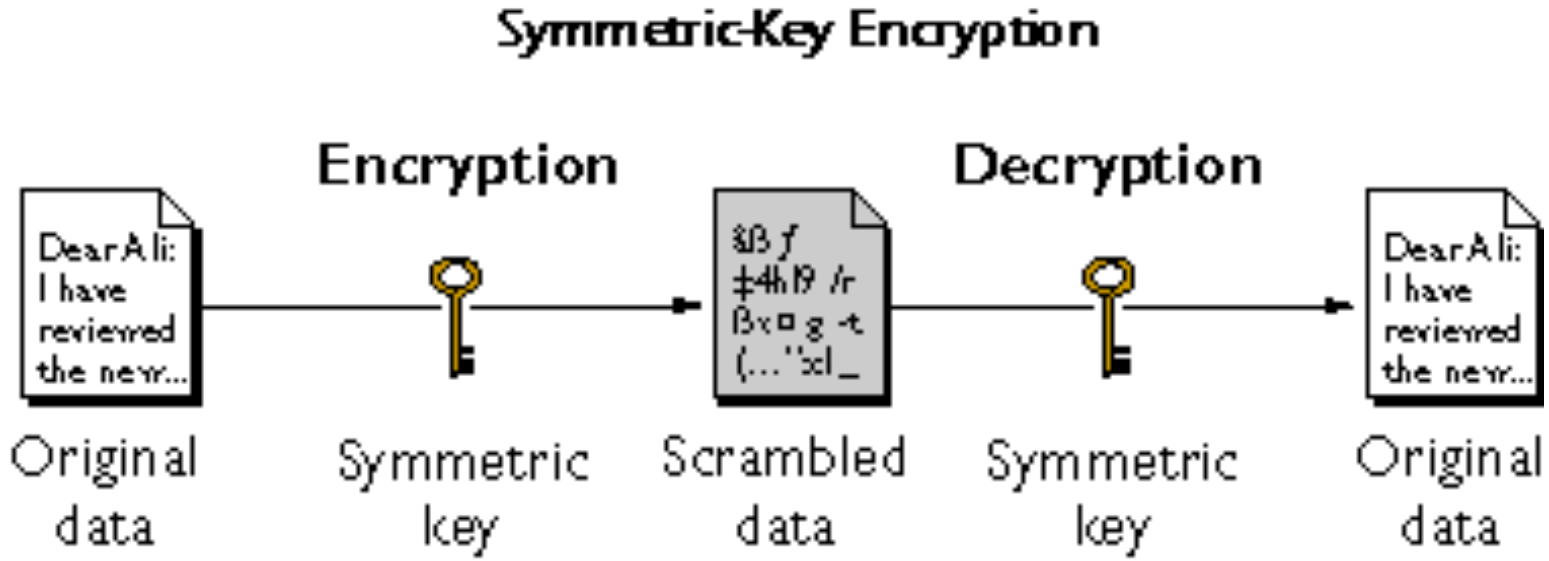
- Integrity
  - Has the data been tampered?
- Confidentiality
  - Has the data been disclosed?
- Authenticity
  - Has the data been forged?
- Non-repudiation
  - Can the data author be proven?

Block vs Stream Ciphers

- Stream Ciphers
  - Best for – Network streams
  - Typically faster
  - Low memory Requirements
  - Does not encrypt whole data blocks at a time
  - No integrity or authentication
- Block Ciphers
  - Best for – Cases where amount of data is pre-known/set
  - Slower
  - Require more memory
  - More susceptible to noise in transmission (whole blocks at a time encrypting)
  - Some have integrity and authentication

Symmetric Key Cryptography

- A **single secret shared** key for encryption and decryption



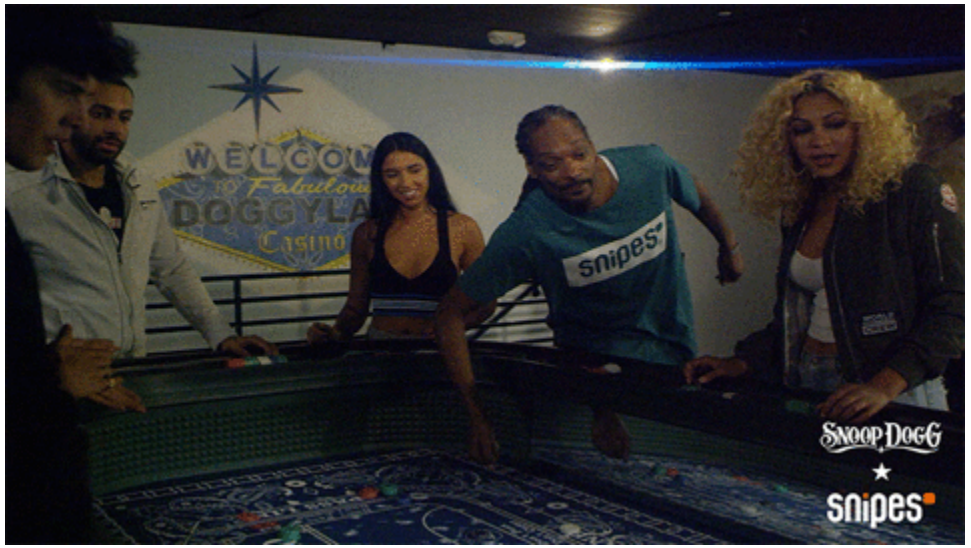
Copyright IBM - https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html

Symmetric Key Cryptography

- Advantages
  - Fast and simple computations
  - Effective confidentiality
  - Strong algorithms that are normally only cracked through “brute force”
  - Good for bulk data
- Disadvantages
  - Difficult to securely store and share the secret key
  - Often lacks authentication and data integrity
  - Data retention cases require key retention which can result in many secret keys

Cryptographic Key Generation

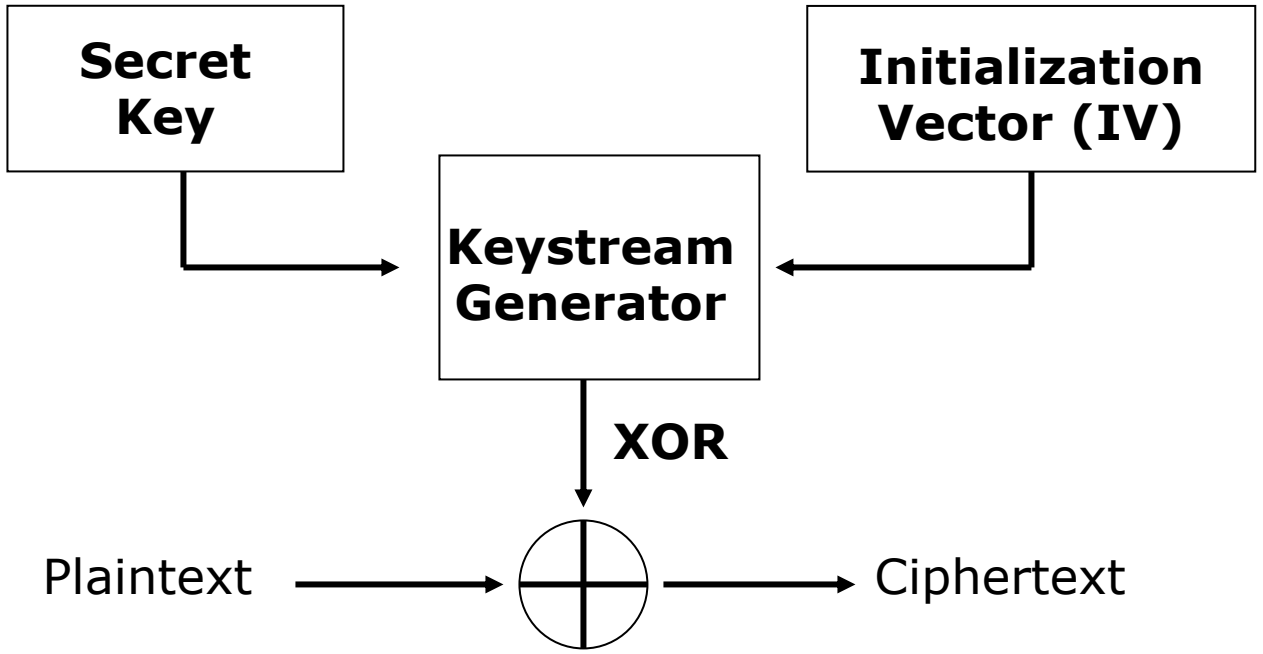
- A cryptographic key is the secret which keeps the secrets secret
- Cryptographic keys must be
  - Kept secret and secure
  - Chosen randomly from the entire key space
  - Unrelated to past or future keys
- It is hard to generate random numbers….



Symmetric Stream Ciphers

- Operate on one bit at a time
- Converts a single symmetric key into a keystream as long as the message
- One bit of plaintext is XOR’ed with one bit of keystream
- Keystreams must never be reused
- Encryption and decryption are typically identical

Symmetric Stream Ciphers



Symmetric Block Ciphers

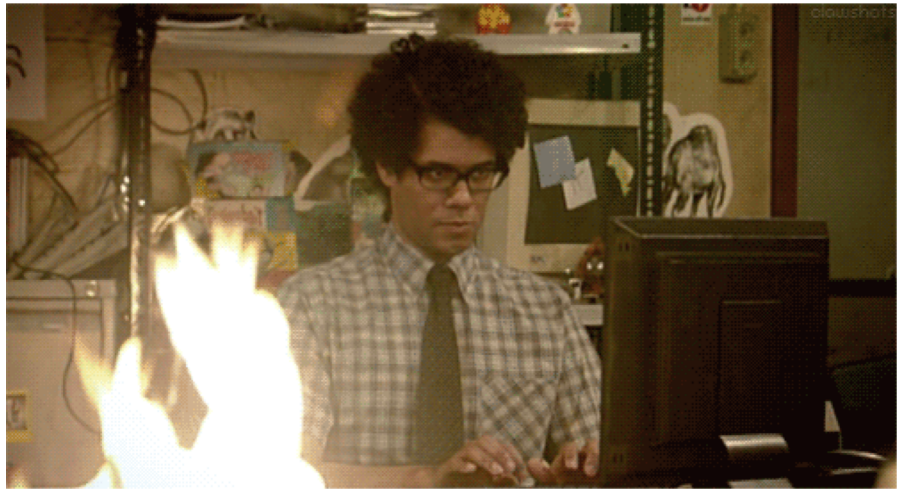
- Operates only on fixed-size blocks of data
- Most block ciphers use simple operations such as addition, multiplication, substitution, permutation and XOR
- The operations are repeated in rounds which each have their own key (subkey), derived from the original secret key

Symmetric Block Ciphers

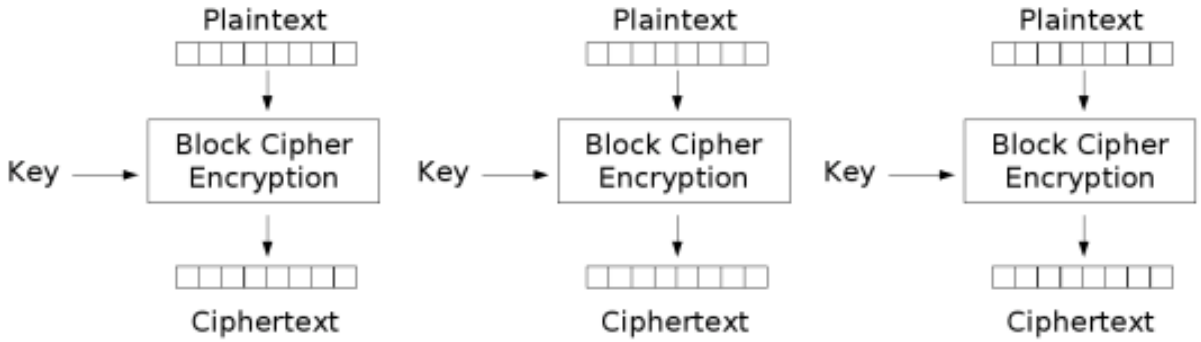
Cipher	Key size (bits)	Block size (bits)	Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14
DES	56	64	16
Triple DES	168	64	48 (16 X 3)

Other Block Cipher Problems…

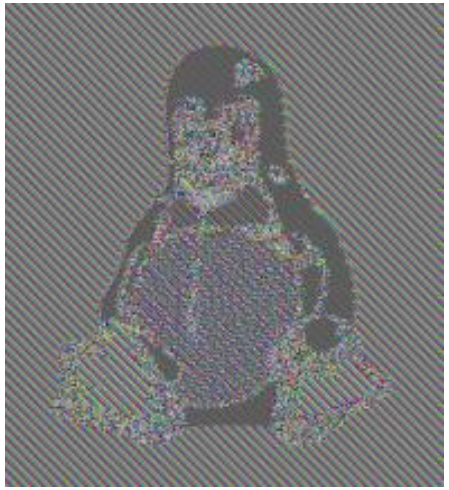
- Each block of plaintext has a defined corresponding cipher text
- Patterns remain as every block of ciphertext represents one block of plaintext
- Because each block gets decrypted in exactly the same way attackers can send the same cipher text over and over (replay attacks)
- No integrity protection
- No authentication



Patterns in Cipher text



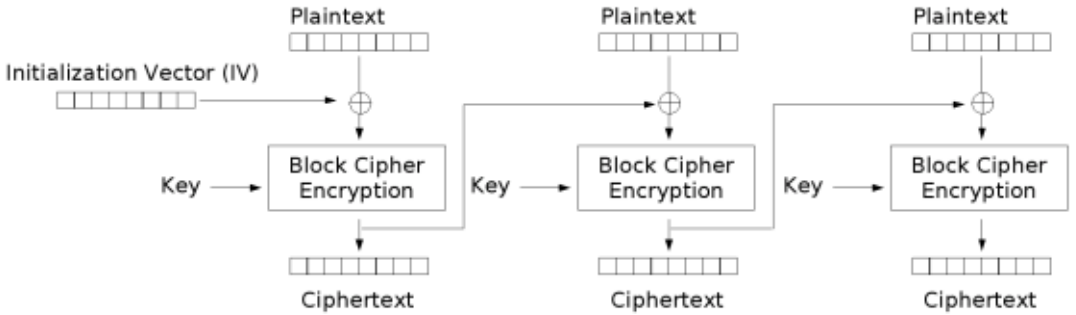
Electronic Codebook (ECB) mode encryption



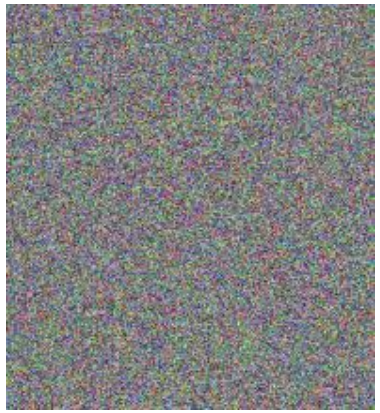
Block Cipher Modes of Operation

- A block cipher always has a mode of operation
- The simplest mode is direct use of the cipher called Electronic Code Book (ECB)
- Modes were introduced by NIST to provide additional properties such as
  - Elimination of patterns in the cipher text
  - Streaming modes for block ciphers
  - Parallelizability (working on two or more blocks at the same time)
  - Random access to operate on an arbitrary block

Block Cipher Modes of Operation
Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption



Symmetric Key Cryptography

- Symmetric key cryptography is extremely difficult to scale, due to the exponential growth in key pairs

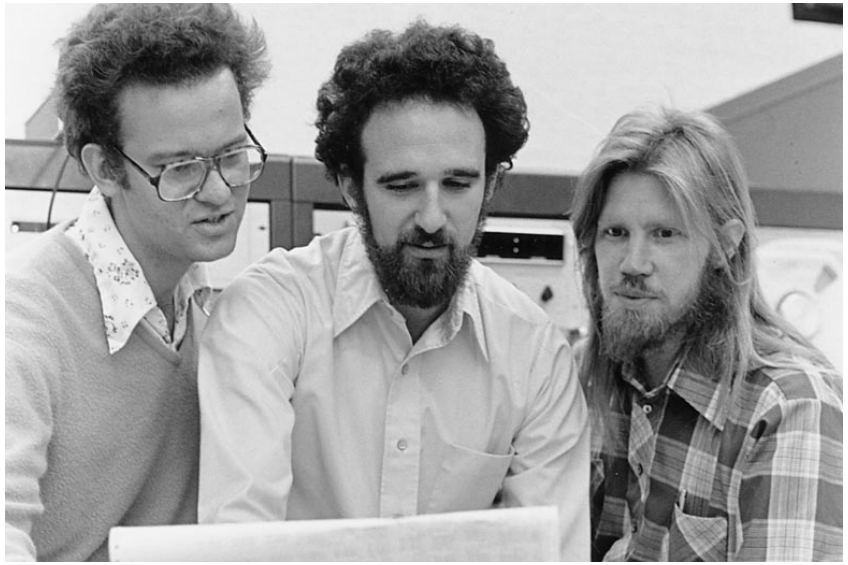
Number of parties	Number of key pairs
2	1
3	3
5	10
10	45
50	1,225
100	4,950
1,000	499,500
263,900	34,821,473,050

Remember the Pros/Cons

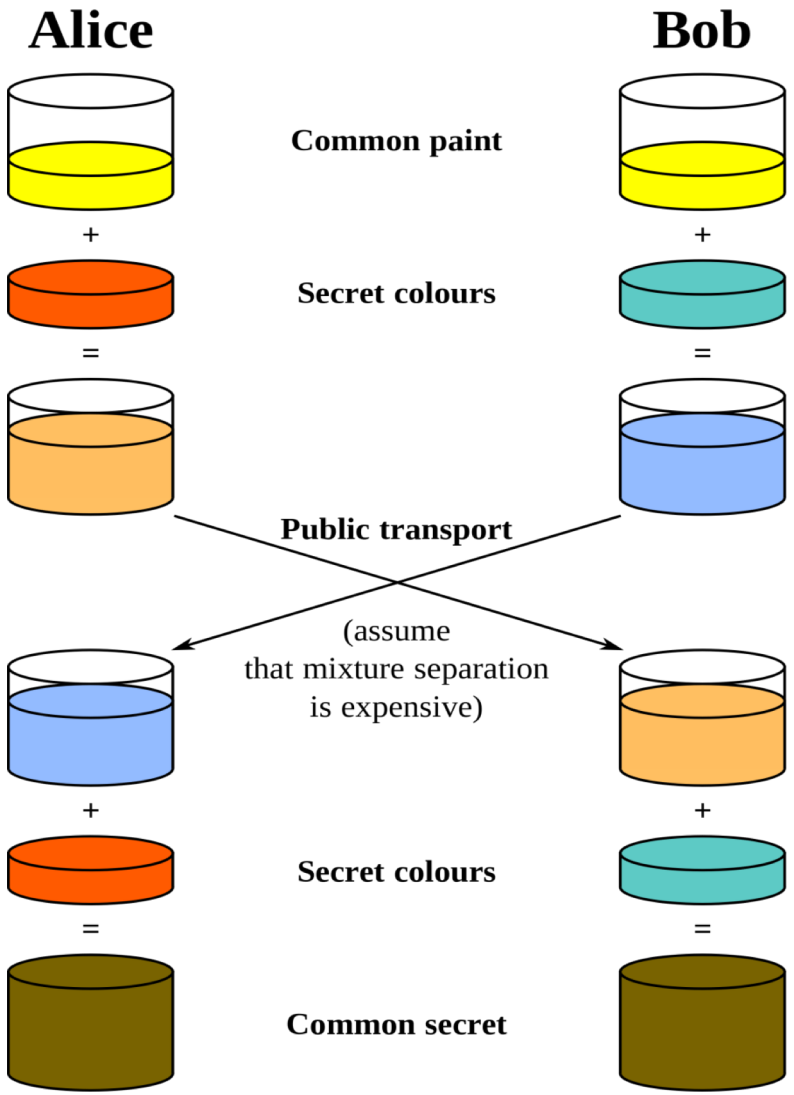
- Advantages
  - Fast and simple computations
  - Effective confidentiality
  - Strong algorithms that are normally only cracked through “brute force”
  - Good for bulk data
- Disadvantages
  - Difficult to securely store and share the secret key
  - Often lacks authentication and data integrity
  - Data retention cases require key retention which can result in many secret keys

Diffie-Hellman Key Exchange

- A method which allows two parties to jointly establish a shared secret key over an insecure communications channel
- Diffie-Hellman raises one number to the power of a second number
- The security depends on the difficulty of reversing the exponentiation



Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange

- The problem with DH is lack of authentication
  - How does Alice know that she is talking to Bob, and not somebody pretending to be Bob?
- A man-in-the-middle could substitute his key during the key exchange, and Bob and Alice would not know

Asymmetric Key Cryptography

- Based on a group of one-way mathematical functions known as “trapdoor functions”
- Each user has a pair of mathematically related keys – one public, one private
- Called “asymmetric” because one key encrypts, the opposite key decrypts
- Also called “public-key cryptography”

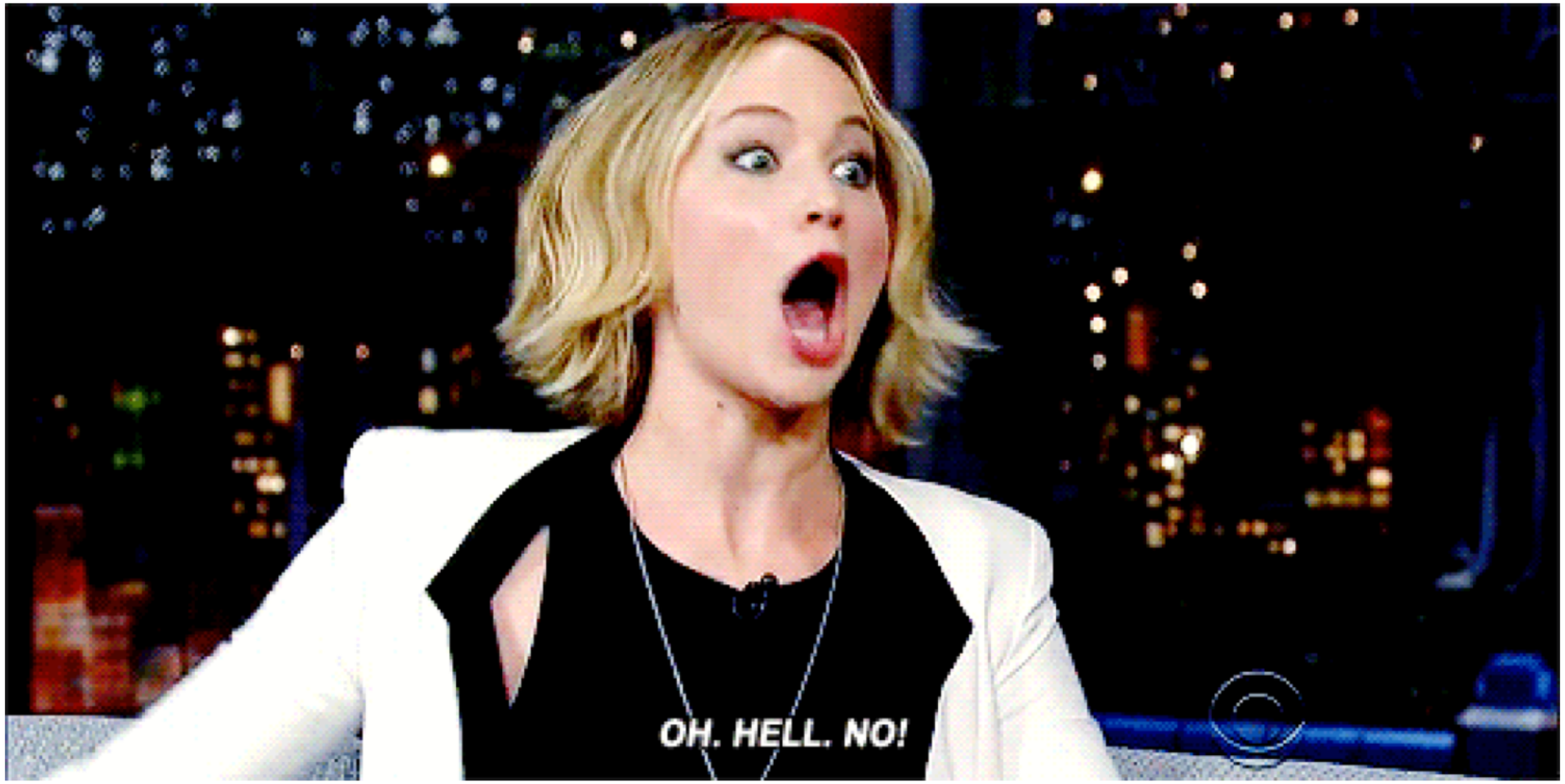
Asymmetric Key Cryptography

- The private key is computationally infeasible to derive from the public key
- The private key must be kept secret
- The public key is not confidential or sensitive to disclosure because the private key cannot be derived from it

Asymmetric Key Cryptography

- Asymmetric keys are typically hundreds of digits
  - 1024 bit keys are over 308 digits
  - 2048 bit keys are over 616 digits
- Typical keys must be very, very large
  - 4096 bit and 3072 bit keys are in use
  - 2048 bit keys are common
  - 1024 bit keys or less should no longer be used
- This compares to 128 to 256 bits, for modern symmetric keys

We are going to do some math…..
Don’t worry. We got this!



RSA – Rivest, Shamir, Adleman

- Inspired by a paper from Diffie, invented by
  - Ron Rivest, Adi Shamir, Leonard Adleman
- Widely used
  - Digital signatures
  - Key distribution
- RSA generates keys by taking two large prime numbers, multiplying them together and combining them with a pair of exponents
  - The product of the two primes as well as one of the exponents are what makes up the “public key”
- The security of RSA depends on the difficulty of finding those prime factors

Simple RSA - How do we keep |G| a secret?

- Setup: p,q primes, n=p*q, $G = (\mathbb{Z}/\mathrm{n}\mathbb{Z})^*$, e, gcd(e, |G|)=1
  |G| = (p – 1)(q – 1)
- Public Key: (n,e)
- Secret Key: $d = e^{-1} mod(p\ -1\ )(q\ -1)$

- Relies on integer factorization for security
- Only know way to keep |G| secret – all rely on factorization problem

Example Math

- **Encryption**
- $F(m,e) = m^e \bmod n = c$

- We need to know all the variables!!

Example Math – Find n

- **Encryption**
- F(*m*,*e*) = m^e mod *n* = *c*

- *n = p * q*
- *Let's pick 7 and 17 for p and q*

- *n = p*q = 7*17 = 119*

Example Math – Find n

- **Encryption**
- $F(m,e) = m^e \bmod n = c$
- *n = 119*

- *Originates from Euler's theorem*
- $\phi(n) = (p-1)(q-1) = 96$

Example Math – Find n

- **Encryption**
- $F(m,e) = m^e \bmod n = c$
- $n = 119$
- $\phi(n) = (p-1)(q-1) = 96$

- ***e*:** 7 -- found by picking a prime value, then running it through the Extended Euclidian Algorithm.

More Example Math

- **Encryption**
- F(*m*,*e*) = m^e mod *n* = *c*
- ***p*:** 7
- ***q*:** 17
- ***n* = *q* x *p*:** 119
- ***φ*(*n*) = (*p*-1)(*q*-1)**: 96
- ***e*:** 7

- *Take the derivative of both sides (calculus)*
- ***d* (*e* x *d* = 1 mod *φ*(*n*)):** 7x = 1mod96 = 55

More Example Math

- **Encryption**
- F(*m*,*e*) = m^e mod *n* = *c*
- ***p*:** 7
- ***q*:** 17
- ***n* = *q* x *p*:** 119
- ***φ*(*n*) = (*p*-1)(*q*-1)**: 96
- ***e*:** 7
- ***d* (*e* x *d* = 1 mod *φ*(*n*)):** 7x = 1mod96 = 55

- Now we have all the variables! We just need a public key (m) to encrypt to. Let's make it 7.

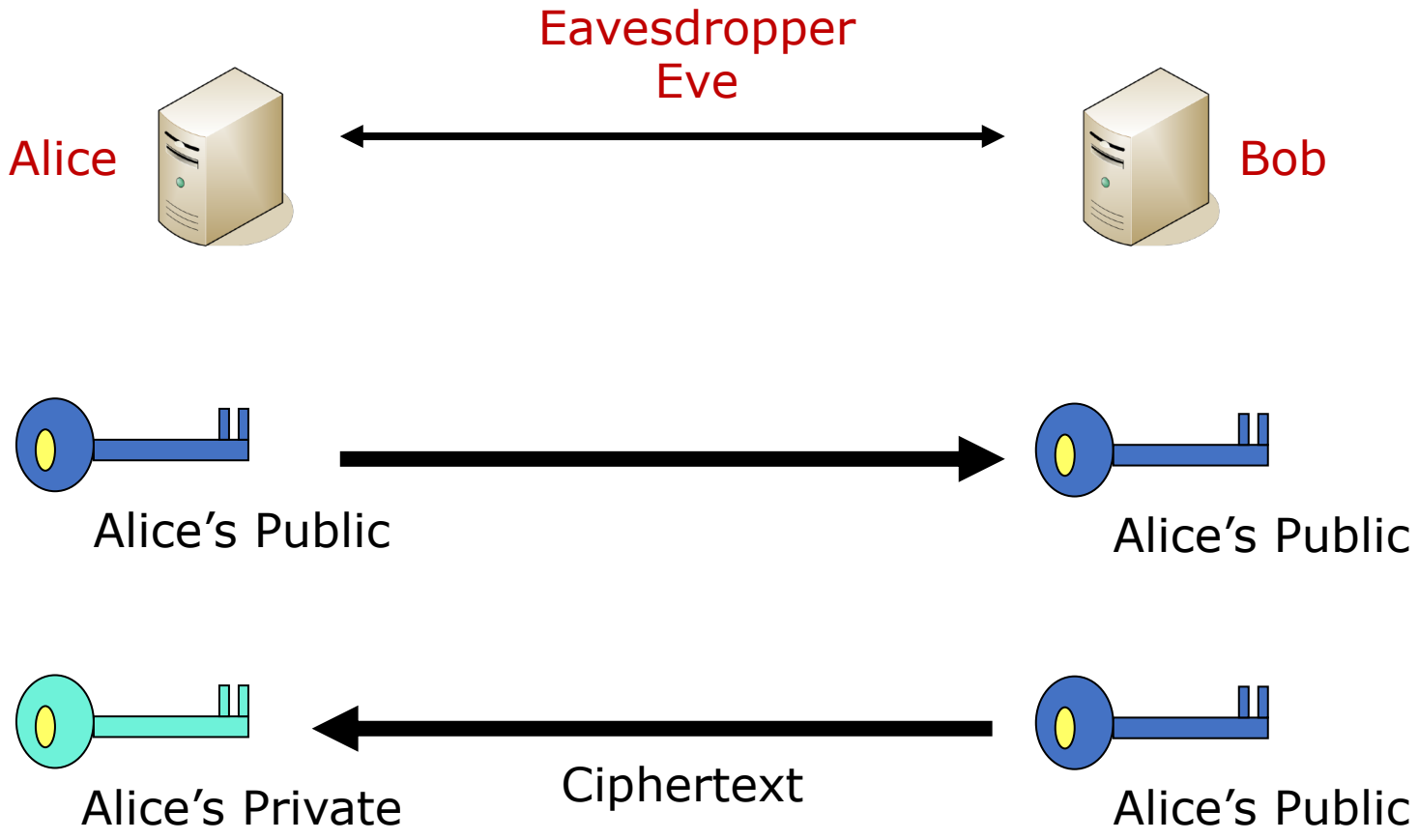
More Example Math

- **Encryption**
- F(*m*,*e*) = m^e mod *n* = *c*
- ***p*:** 7
- ***q*:** 17
- ***n* = *q* x *p*:** 119
- ***φ*(*n*) = (*p*-1)(*q*-1)**: 96
- ***e*:** 7
- ***d* (*e* x *d* = 1 mod *φ*(*n*)):** 7x = 1mod96 = 55

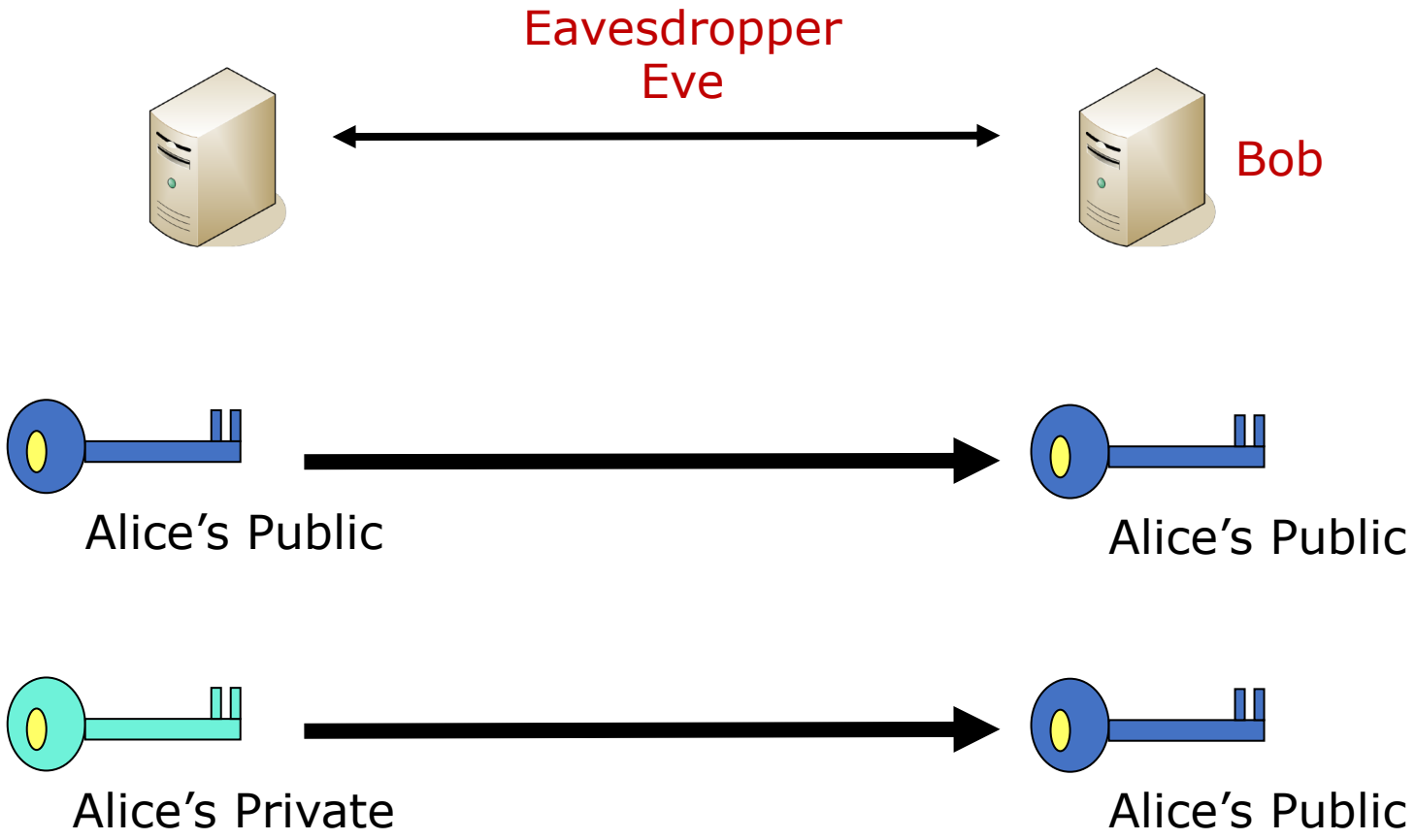
- m=7
- 7^7 mod 119 = 63 = c

We just encrypted something using math :D

Confidentiality: Keeping Secrets

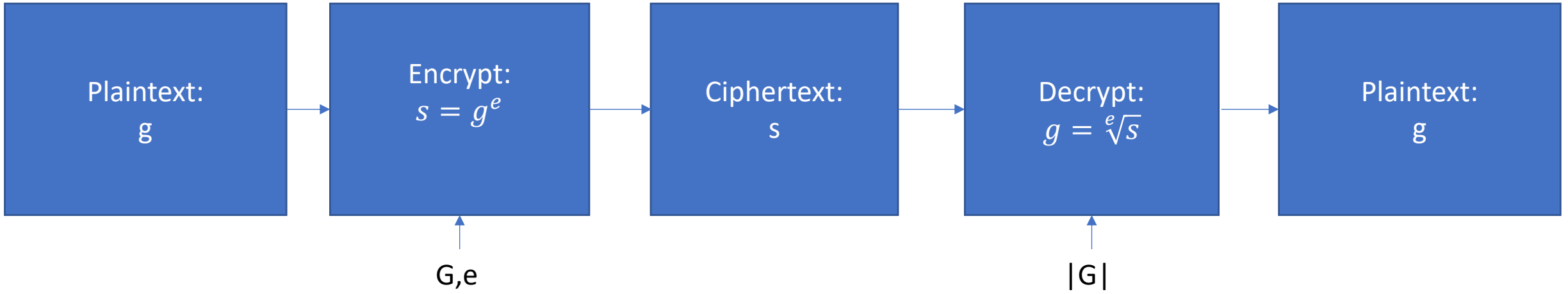


Authenticity: Verifying the Sender



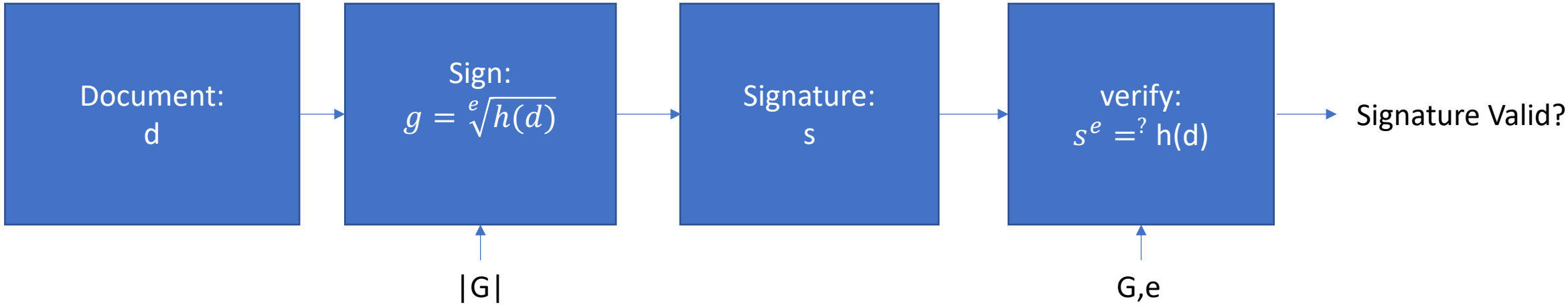
Less Complex Simple RSA Encryption Math Explanation

- Public Key: finite Group $\boldsymbol{G}$, exponent $\boldsymbol{e}$, gcd($\boldsymbol{e}$,|$\boldsymbol{G}$|)=1
- Secret Key: |G|
- Allows to compute: $\sqrt[e]{g} = g^{e^{-1} * mod|G|}, g \in G$



Less Complex Simple RSA Signing Math Explanation

- Public Key: finite Group ***G***, exponent ***e***, gcd(***e***,|***G***|)=1
- Secret Key: |G|
- Allows to compute: $\sqrt[e]{g} = g^{e^{-1} * mod|G|}, g \in G$
- Hash function: h: {0,1}* -> G



ECC – Elliptic Curve Cryptography

- Gaining Popularity
- Digital signatures (ECDSA)
- Key exchange (ECDHE)
- Can use smaller keys for comparable security
- Smaller keys come with significant performance increases

Asymmetric Key Security - Classical

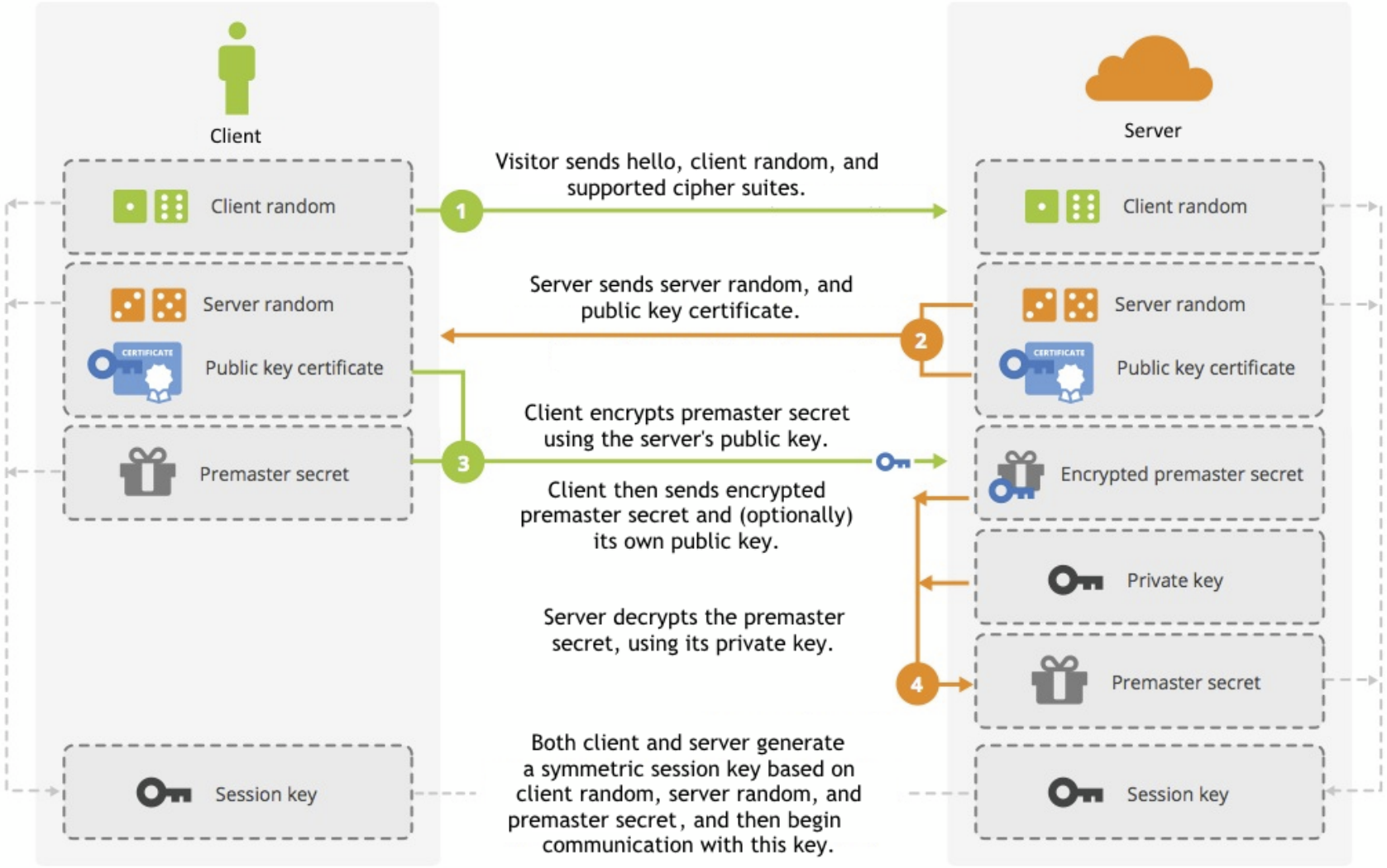
Secure Until	Security Level	RSA modulus	Elliptic Curve
Obsolete Recently – 2015	80	1248	160
2025	96	1776	192
2030	112	2493	224
2040	128	3248	256

* Without quantum available

Asymmetric Key Cryptography

- Advantages
  - Can provide confidentiality (encryption)
  - Can provide authentication of origin
  - No key distribution problem to solve
- Disadvantages
  - Computationally intensive
  - Usually needs really large keys
    - 2048 bits or higher
    - ECC can be secure with keys of 256 bits or higher

Transport Layer Security (TLS) Secure Socket Layer (SSL) Handshake



Perfect Forward Secrecy

- The TLS handshake in the previous slide used RSA both for the key exchange and for the authentication
  - Very fast!
  - Somebody can simply record this -- and all other -- fully encrypted conversations
  - Future keys can decrypt the past
- DHE (Diffie-Hellman Ephemeral) key exchange solves this issue
  - You still use RSA for authentication, but you use Diffie-Hellman to determine the symmetrical keys for each connection
  - Once the transaction is completed, you throw away these keys, protecting your transaction forever

Questions? – Anthony.Kosednar@gmail.com

Future talk…..

Post Quantum Cryptography & Quantum Resistant Algorithms - The threat of Shor’s Algorithm with qubits and the obsoleting of modern cryptography in the next 10 years.

Hopefully with less factorization and polynomials ;)