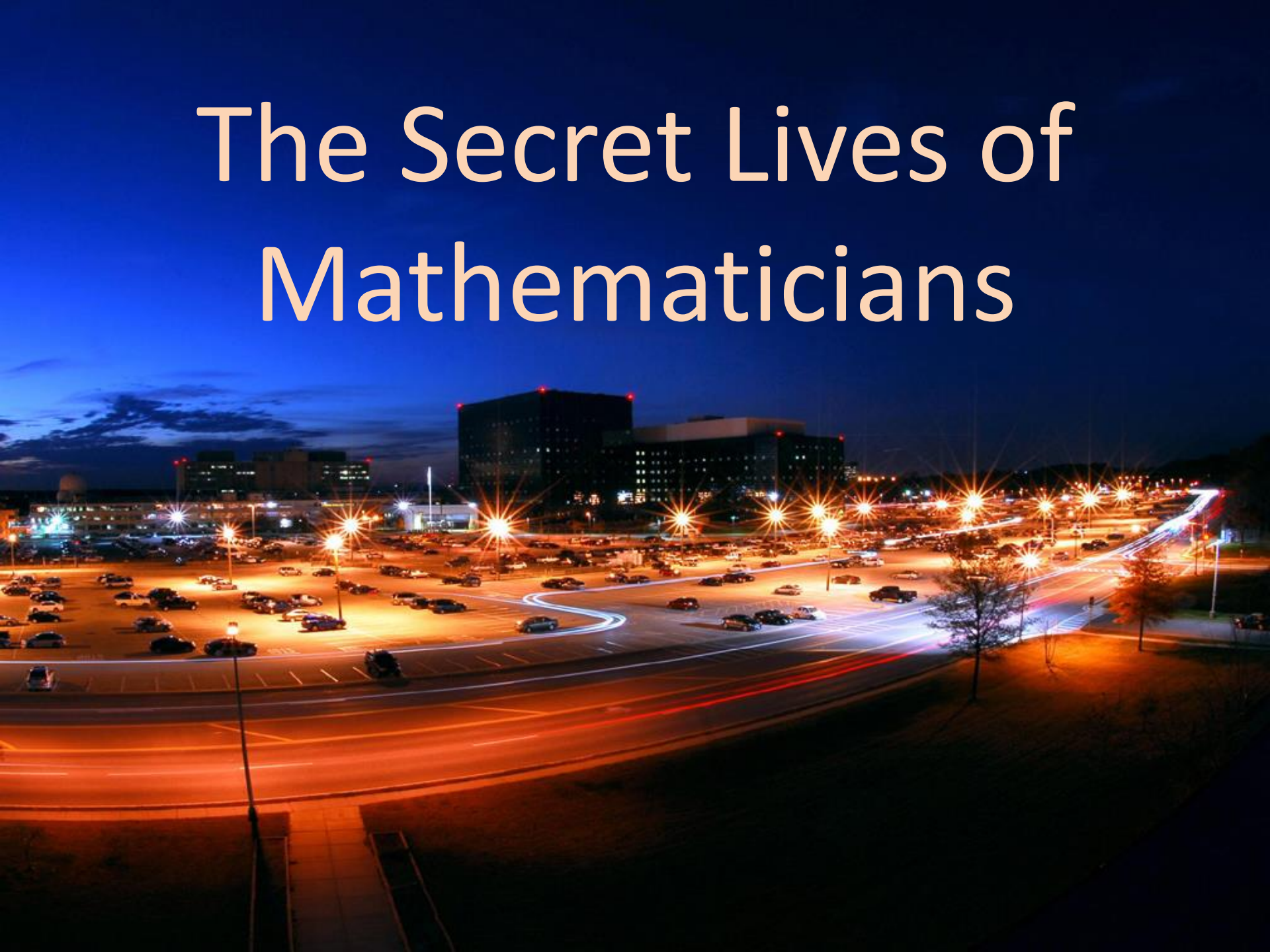
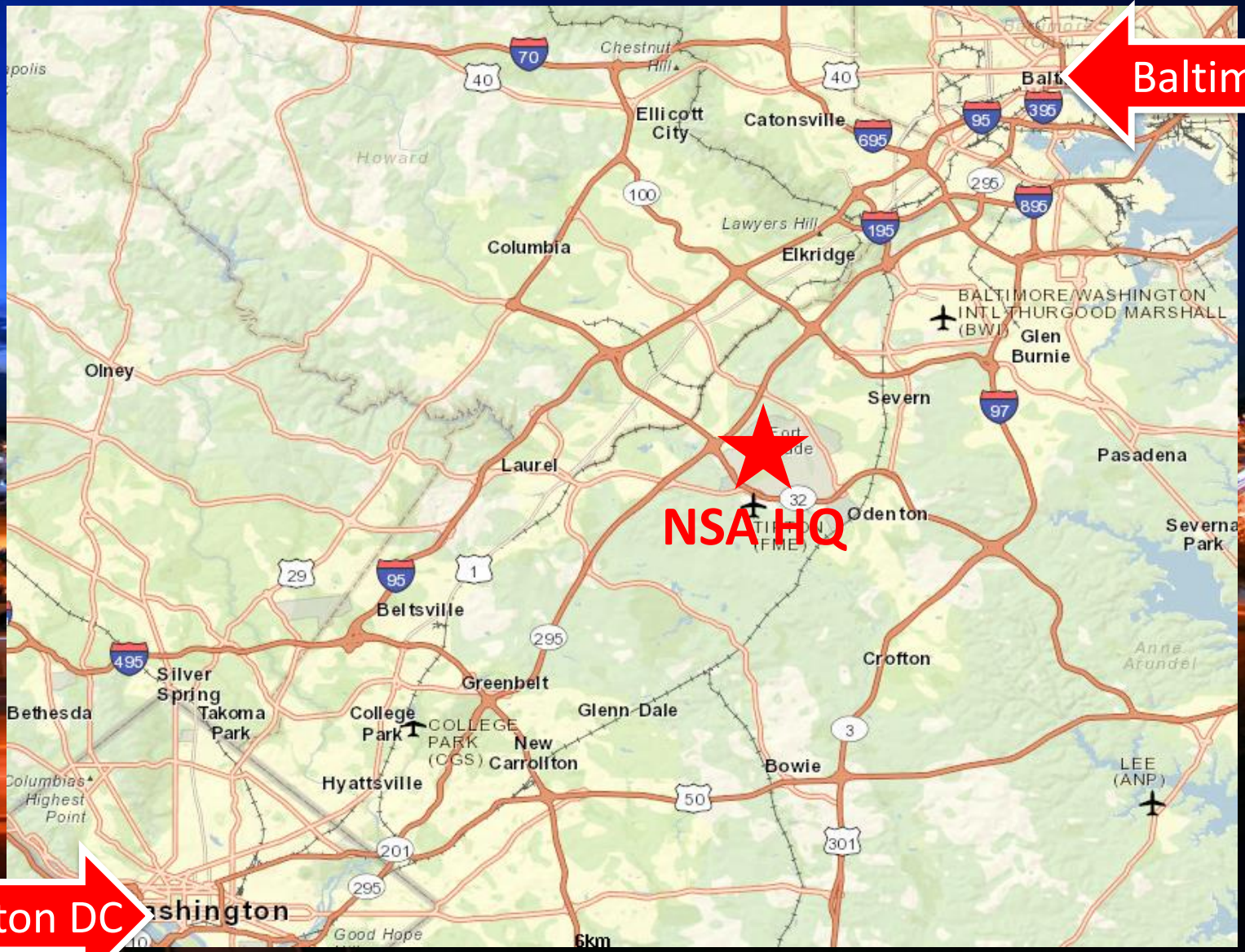
The Secret Lives of Mathematicians



Where in the World?



History of **N**o **S**uch **A**gency

Before the NSA:

- Codes were handles by Armed Forces Units
- WWI and WWII brought a higher need for cryptologic concentration

Establishment:

- Created November 1952 by President Truman
- Centralized and joined military and civilian Cryptologic Activity into one organization

What You May Have Heard…

What You May Have Heard…

Books

- Digital Fortress by Dan Brown
- Red Storm Rising by Tom Clancy

Movies

- Enemy of the State (1998)
- xXx (2002): Vin Diesel
- The Simpsons Movie (2007)

TV

- Scandal
- NCIS: Eleanor 'Ellie' Bishop
- Person of Interest
- Chuck: John Casey

Who Are We Really?

Who Are We Really?

- Civilians
- Military
- Lawyers
- Engineers
- Mathematicians
- Language Analysts
- Accountants
- Computer Scientists
- Management
- And More!!!

What We Really Do…

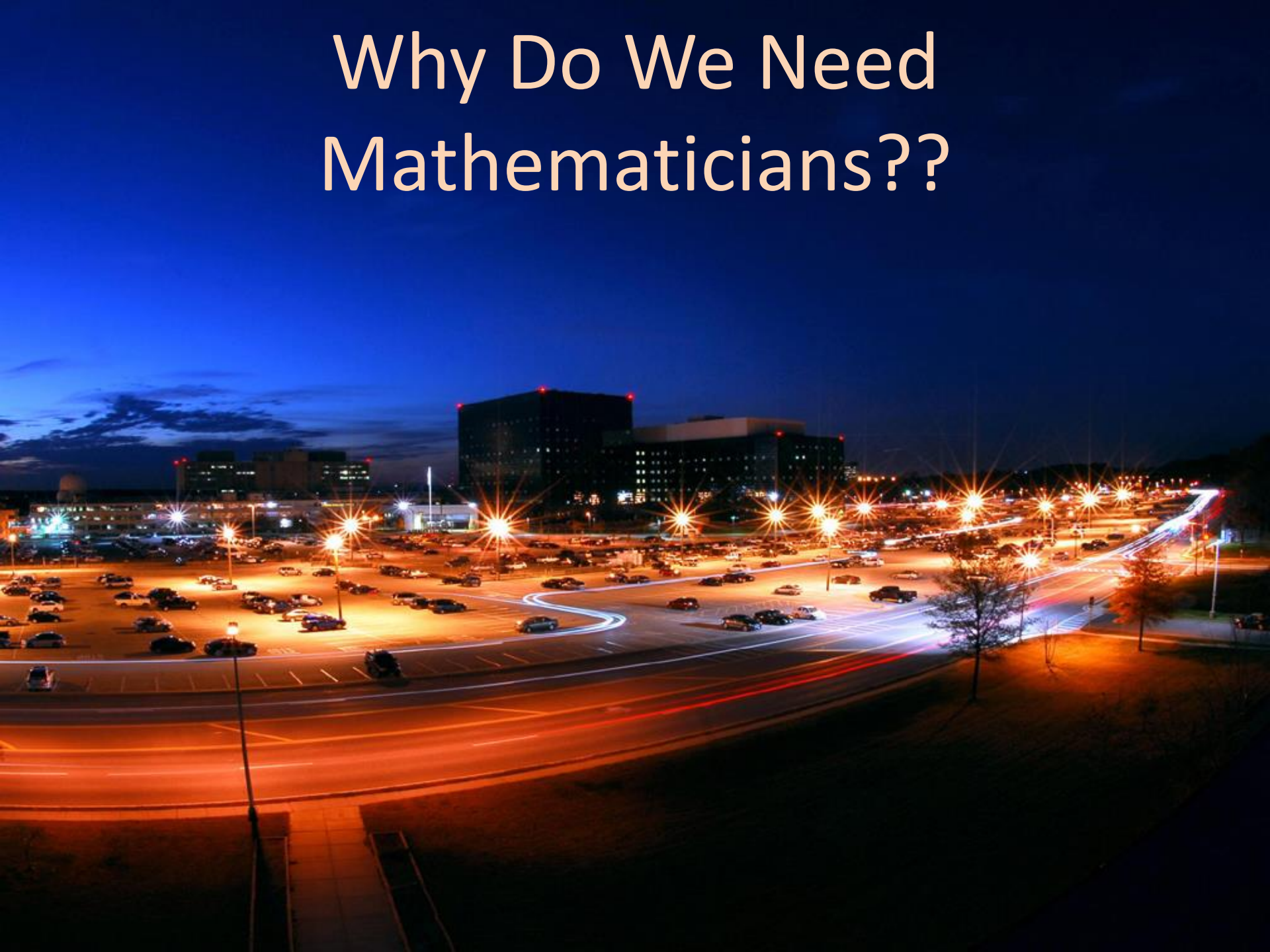
What We Really Do…

- Workforce Support Activities ★
- Business Management and Acquisition
- Engagement & Policy
- Research ★
- Capabilities ★
- Operations ★

What We Really Do…

- Research
  - Manages research on developing capabilities
  - The "Really Big" Problems
- Capabilities
  - Develops and provides solutions
- Operations
  - Executes all operations, analysis, and information
  - Signals Analysis, Information Assurance, and Cyber Defense

Why Do We Need Mathematicians??



The Role of Mathematicians

We Use:

…Number Theory, Group Theory, Graph Theory, Linear Algebra, Math Modeling, Probability and Statistics, Combinatorics…

In Combination With:

… computer science, data processing techniques, advanced technology…

To:

…search for weaknesses in adversaries' systems

… build and strengthen national systems

… research, discover, and develop new security techniques

What are the Mathematicians Doing?

They Work in:

- Computer and Network Security
- Signals Analysis
- Data Mining
- Information Retrieval
- Information Processing
- Speech Processing
- Analysis of Computer Networks
- Data Compression
- Super Computing
- Biometrics
- And much, much more!

How Do You Fit In??

How Do You Fit In?

Workforce Support Activities

Career Development Programs

- AMP
- CMP
- CADP
- C2DP
- SADP
- And More!

3 Year Training Programs with:

4-6 Rotational Tours
One-the-job Classes
Senior Leadership and Mentoring
Permanent Placement Upon Completion

Summer Opportunities

PROGRAM	MAJOR(S)		UNDERGRAD ELIGIBILITY	GRADUATE ELIGIBILITY
Cryptologic Access Summer Intern Program (CAP)	• Mathematics • Computer science	• Computer/electrical engineering • Telecommunications	✔	
Director's Summer Program (DSP)	• Mathematics	• Other majors with a minor in mathematics or a strong math curriculum	✔	
Cryptanalysis and Exploitation Services Summer Program (CES SP)	• Mathematics • Other majors with a strong background in mathematics	• Computer science	✔	
Graduate Mathematics Program (GMP)	• Mathematics			✔
Summer Program for Operations Research Technology (SPORT)	• Computer science • Computer/electrical engineering	• Network engineering • Mathematics • And others		✔

12 Week Paid Internships!
Deadlines typically in mid-October

Top 10 Reasons to Work at NSA

Top 10 Reasons to Work at NSA

10) Large Expert Community (collaboration and mentoring are highly encouraged)

9) Casual Dress Code

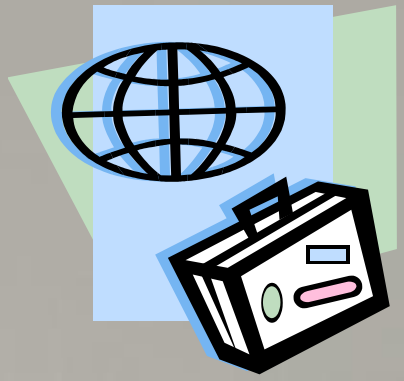
8) Excellent Benefits (Health, Retirement, Vacation/Sick)

7) Flexible Schedule

6) NSA Supports Furthering Education

Top 10 Reasons to Work at NSA

5) Opportunities to Travel



4) Diversity of Work

3) Impact

2) Challenging and Fun

And…

Top 10 Reasons to Work at NSA

1) … You'll never turn a Happy Hour into a Sad Hour by talking about work!

Application Requirements

Application Requirements

One must:

- Be a US Citizen
- Be able to obtain a TS Security Clearance (includes background investigation, polygraph, and psychological evaluation)
- Allow 6 to 18 months for application processing

What is Cryptanalysis?

Definitions

Plaintext: Text or file which will be encoded

Cipher Text: Encoded plaintext

Code: Replaces elements of a plaintext by other letters, numbers, words, or symbols

Cipher: Transposes or substitutes elements of plaintext according to a key

Definitions

Cryptanalysis: The decryption of messages into plaintext without having initial knowledge of the key used to encrypt

Cryptography: The science and art of making codes and ciphers

Cryptology: The science and art of making AND breaking codes and ciphers

Definitions

What is a character?

Binary: base 2: (uses 2 distinct symbols) 0 and 1
Each symbol represents 1 bit

This is the "language" a computer uses to talk

Hex: base 16 (uses 16 distinct symbols): a-f and 0-9
each symbol represents 4 bits

ASCII: printable characters (all the letters, numbers, and symbols on these slides)
each symbol represents 8 bits or 1 byte

Definitions

What is a character?

0100001101110010011110010111000
0011101000110000101101110011000
0101101100011110010111001101101
00101110011

Definitions

What is a character?

01000011011100100111100101110000
00111010001100001011011100110000
01011011000111100101110011011010
00101110011

0x4372797074616e616c79736973

Definitions

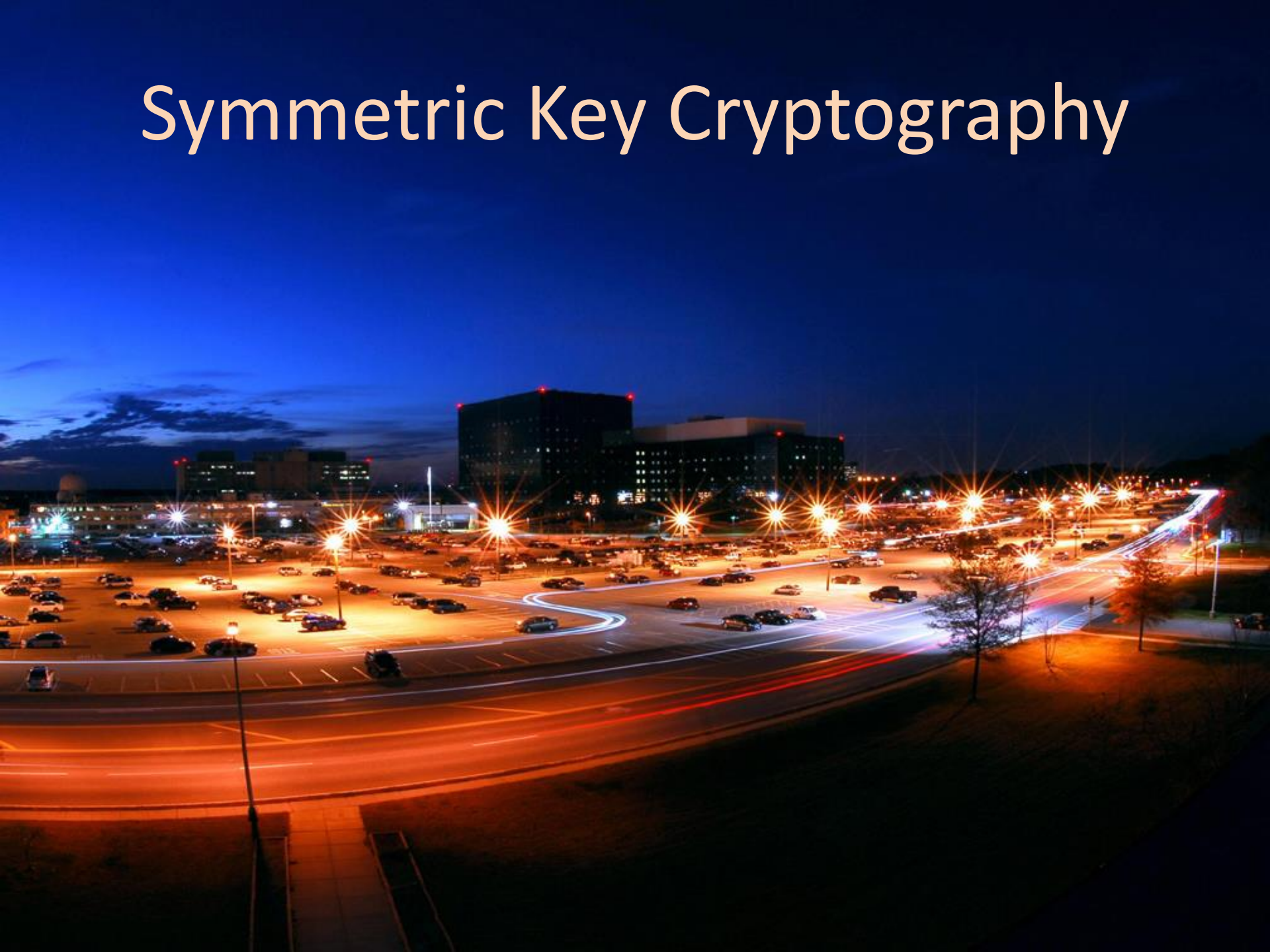
What is a character?

01000011011100100111100101110000
0011101000110000101101110011000
0101101100011110010111001101101101
00101110011

0x4372797074616e616c79736973

Cryptanalysis

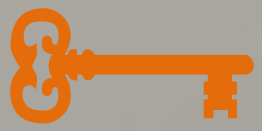
Symmetric Key Cryptography



Symmetric Key Cryptography

The General Idea:

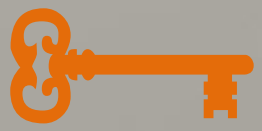
1. Alice sends Bob a message encrypted with key, k
2. Bob decrypts the message with key, k



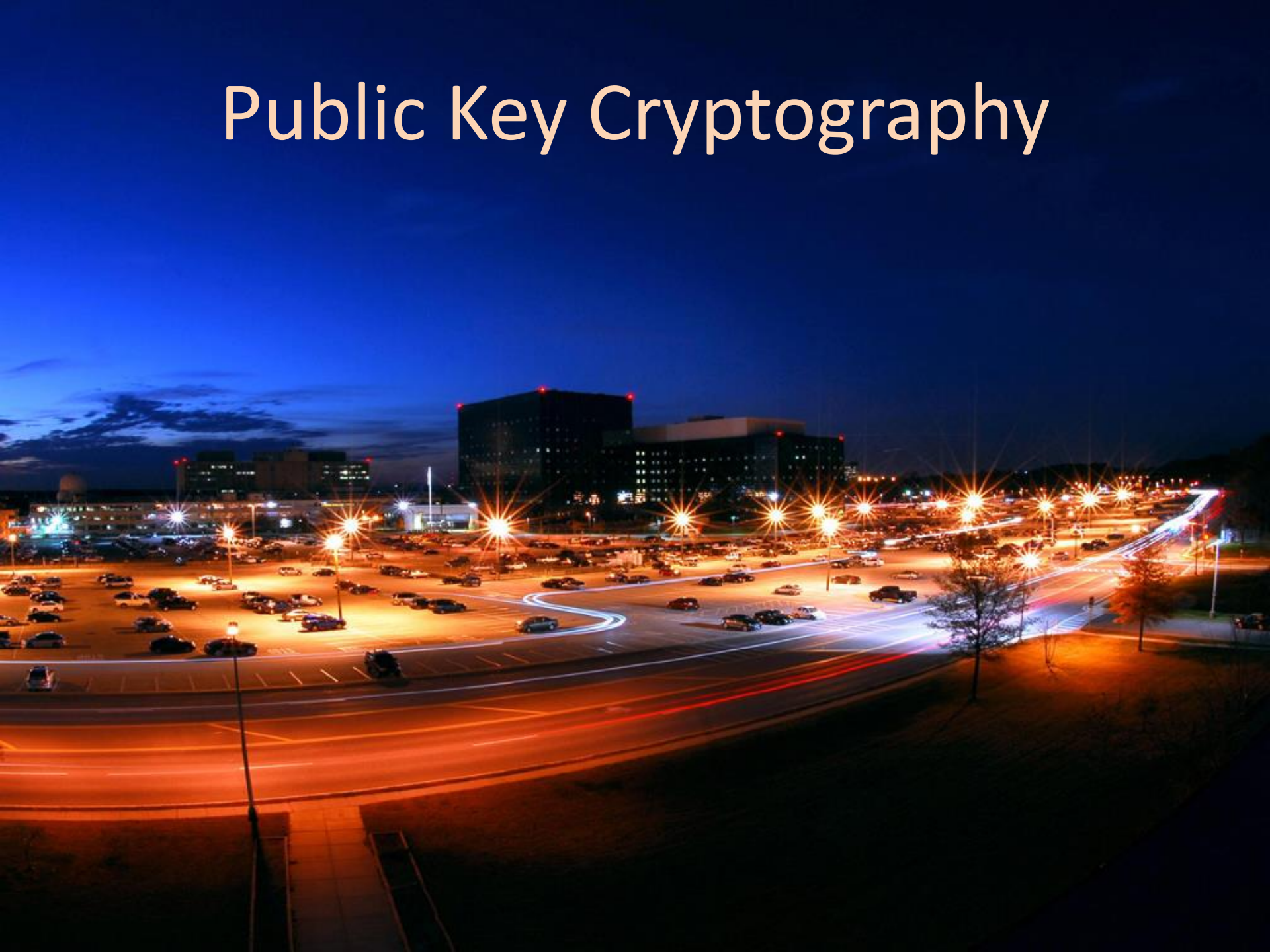
Kerckhoff's Principle

Kerckhoff's Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.



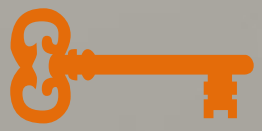
Public Key Cryptography



Public Key Cryptography

The General Idea:

1. Alice and Bob agree on a key system to use
2. Alice and Bob assume Eve could intercept their communication
3. The goal is to get a shared value only they know



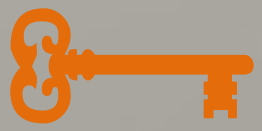
Diffie-Hellman Key Exchange

"The Silent Exchange"

One of the earliest forms of Key Exchange

Originally designed by Ellis, Cocks, and Williamson at GCHQ

Discovered by Diffie and Hellman in 1976



Diffie-Hellman Key Exchange

Secret Values will be in red

Public values (non-secret) will be in purple

p is a large prime

g is a generator of a group or order p

Diffie-Hellman Key Exchange

Alice

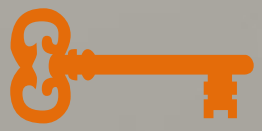
a: Alice's value

$A = g^{a} (mod\ p)$

Bob

b: Bob's value

$B = g^{b} (mod\ p)$



Diffie-Hellman Key Exchange

Alice

a: Alice's value

$A = g^{a} (mod\ p)$

Bob

b: Bob's value

$B = g^{b} (mod\ p)$

$B^{a} = g^{ba} (mod\ p)$

$= K$

$A^{b} = g^{ab} (mod\ p)$

$= K$

Diffie-Hellman Example

$p = 23$ $g = 5$

Alice

a = 6

$A = 5^6 (mod\ 23)$

$A = 8$

Bob

b = 15

$B = 5^{15} (mod\ 23)$

$B = 19$

$K = 19^6 (mod\ 23)$

$= 2$

$K = 8^{15} (mod\ 23)$

$= 2$

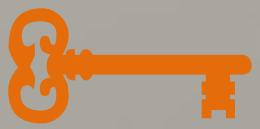
How is Diffie-Hellman Secure?

How is Diffie-Hellman Secure?

When p is large, recovering a from g^a is difficult

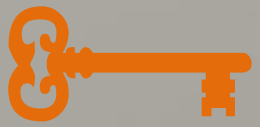
(This is also known as the Discrete Logarithm Problem)

This is why choosing g to be a generator of a group order p is a wise idea.

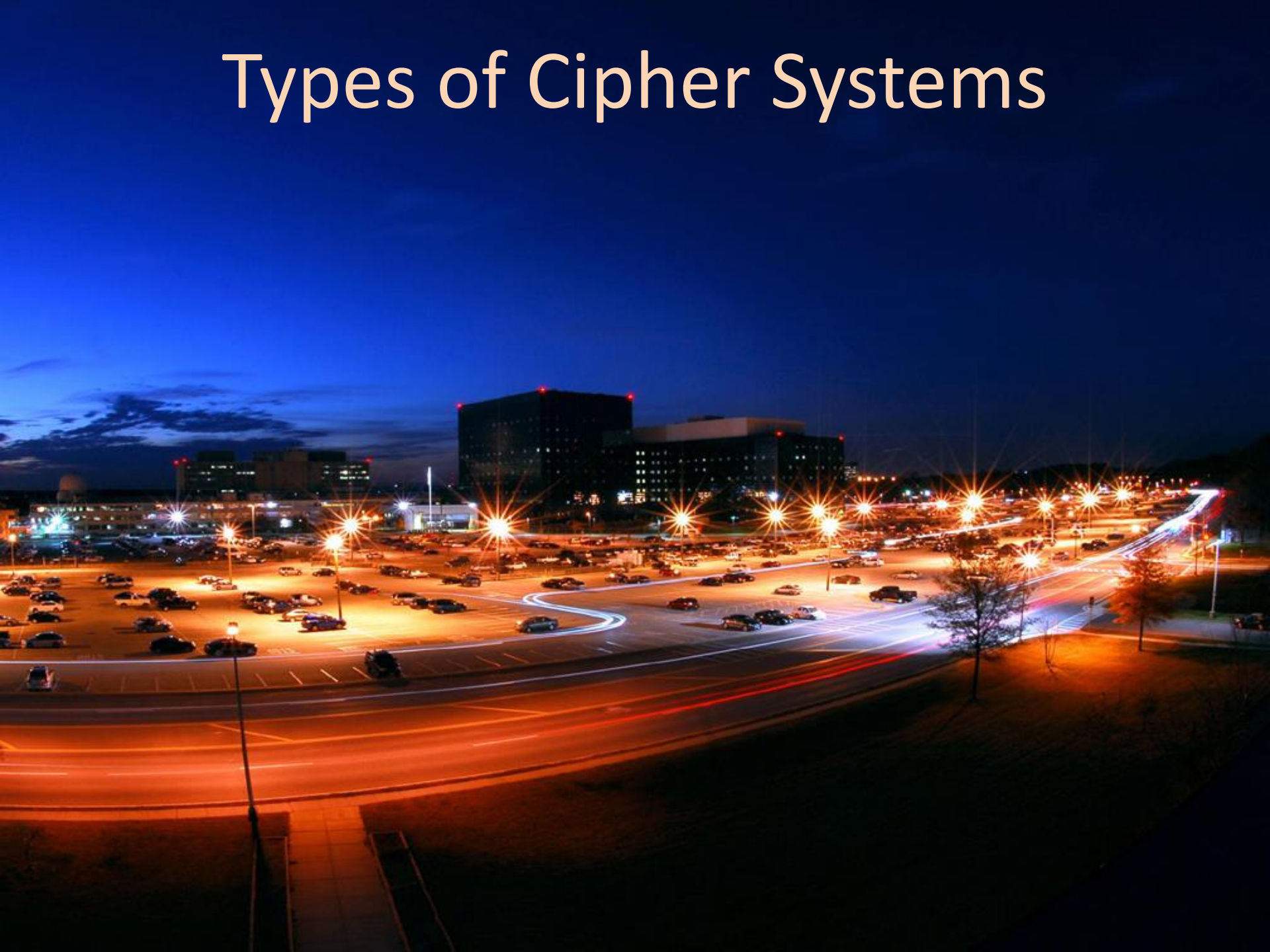


Other Types of Commercial Encryption

- AES: Advanced Encryption Standard (Rijndael cipher)
- DES: Data Encryption Standard
- ECC: Elliptic Curve Cryptography
- PGP: Pretty Good Privacy
- RSA: Rivest, Shamir, and Adleman
- And more!



Types of Cipher Systems



Types of Cipher Systems

Stream Cipher:

- Uses a stream of “random” key called the keystream
- Each plaintext character is combined with a corresponding character of keystream to become cipher
- A character is normally a bit
- Encryption/decryption happens “on the fly”
- Operation to combine bits normally is an XOR

Types of Cipher Systems

Block Cipher:

- 2 paired algorithms (one for encryption and its inverse for decryption)
- Algorithm uses a fixed-length group of characters called a block
- Input is a block size and key size
- Encrypts/Decrypts a block at a time.

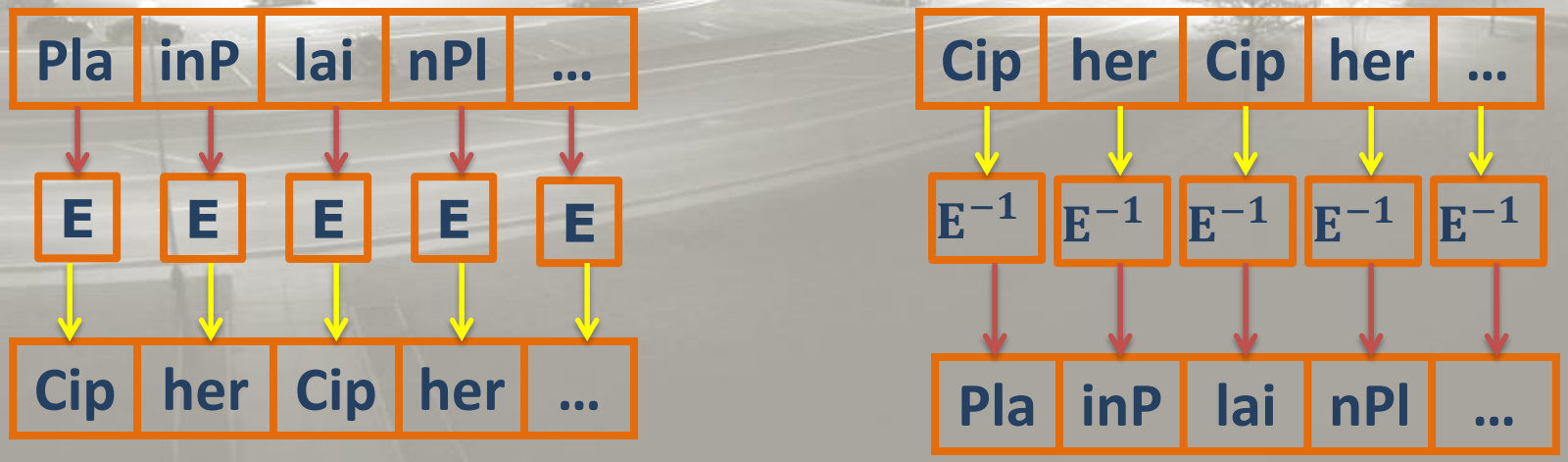
Types of Cipher Systems

Stream

Types of Cipher Systems

Stream

Block



Want More?

www.nsa.gov

Questions?