

So You Want to Break Codes: Careers in Government for Mathematicians

Edray Herber Goins

Department of Mathematics
Purdue University

September 22, 2011



Outline of Talk

- 1 Challenge Problem
- 2 National Security Agency
 - What is NSA?
 - Director's Summer Program
 - Institute for Defense Analyses
 - Center for Communications Research
- 3 What Mathematics Does NSA Do?
 - Shift Cipher
 - ASCII and Unicode
 - Examples
 - Affine Cipher
- 4 Challenge Problem Revisited

Challenge Problem!

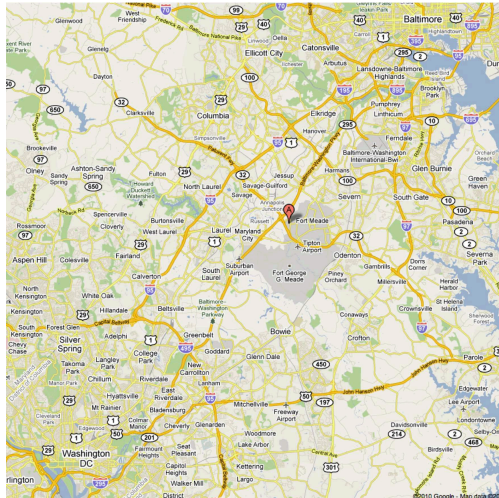
BANJO is to **FERNS**
as
PECAN is to **[?]**

Where Are Such Problems Useful?



National Security Agency

<http://www.nsa.gov/>



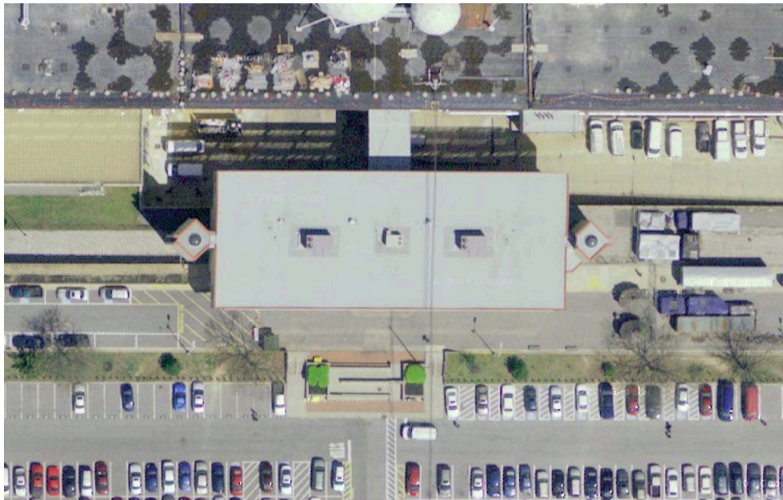
9800 Savage Road, Ft. George G. Meade, MD

http://en.wikipedia.org/wiki/National_Security_Agency



Main Building

http://en.wikipedia.org/wiki/Fort_George_G._Meade



Secure Entrance to Main Building

http://en.wikipedia.org/wiki/Fort_George_G._Meade

Facts About NSA

- The **National Security Agency/Central Security Service (NSA/CSS)** is a cryptologic intelligence agency of the United States Department of Defense responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting U.S. government communications and information systems, which involves cryptanalysis and cryptography.
- NSA's mission is to **collect information that constitutes "foreign intelligence or counterintelligence" while not acquiring information concerning the domestic activities of United States persons.** NSA has declared that it relies on the FBI to collect information on foreign intelligence activities within the borders of the USA, while confining its own activities within the USA to the embassies and missions of foreign nations.
- Largest employer of mathematicians in the world. In fact, NSA has invested many millions of dollars in academic research.

To Work for NSA, Must I Live in Maryland?

Opportunities at NSA

- Director's Summer Program (DSP)
- Institute for Defense Analyses (IDA)
- Center for Communications Research (CCR)
 - Princeton, NJ
 - La Jolla, CA

The screenshot shows the official website of the National Security Agency Central Security Service. The header features the agency's name and the motto "Defending Our Nation. Securing The Future." Below the header is a navigation menu with links to HOME, ABOUT NSA, ACADEMIA, BUSINESS, CAREERS (highlighted in red), INFORMATION ASSURANCE, RESEARCH, PUBLIC INFORMATION, and COMMITMENT. The main content area is titled "Opportunities for YOU" and features a large banner for the "Director's Summer Program (DSP)". The DSP is described as a highly competitive program for undergraduate mathematics majors. A sidebar on the left lists various career and student resources. A "Hot Jobs" section on the right lists Computer Scientists, Computer Engineers, and Electrical Engineers. The page also includes a search bar and a "Contact Us" link.

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE
Defending Our Nation. Securing The Future.

HOME ABOUT NSA ACADEMIA BUSINESS **CAREERS** INFORMATION ASSURANCE RESEARCH PUBLIC INFORMATION COMMITMENT

Home > Careers > Opportunities for You > Students > Undergraduate

Careers
Job Search/Apply Online
How to Apply
~ Opportunities for You
~ Students
High School
+ Undergraduate
Graduate
Professionals
Transitioning Military
College Career Fair Schedule
Career Fields
Student Programs
Life at NSA
Benefits
Career Development
Diversity
FAQs

Director's Summer Program (DSP)

The Director's Summer Program (DSP) is a highly competitive program that seeks to reach the Nation's most outstanding undergraduate mathematics majors. Each summer, we invite exceptional undergraduate students to put their problem-solving skills to the test in mathematics, cryptography and communications technology. These problems often involve applications of Abstract Algebra, Geometry, Number Theory, Probability, Statistics, Combinatorics, Graph Theory, Algorithms, Computer Science and Analysis. State-of-the-art computing resources are available to all students. For the most part, programming is done in C in a Linux environment. Computational algebra packages, including Mathematica, MATLAB, Magma and MAPLE are available, in addition to a variety of statistics packages.

The DSP is looking for students who have distinguished

Where Intelligence Goes to Work®

CollegeGrad.com Top 25

Hot Jobs

- Computer Scientists
- Computer Engineers
- Electrical Engineers

Contact Us
Feedback
E-mail a Friend

Director's Summer Program

http://www.nsa.gov/careers/opportunities_4_u/students/undergraduate/dsp.shtml



Rigorous Analyses • Unquestioned Objectivity

[ABOUT US](#) | [RESEARCH AREAS](#) | [CAREERS](#)



Institute for Defense Analyses

Addressing National Security Issues Since 1956

Careers at IDA

Solving Real World Problems

[View Current Openings](#)

Welcome to the Institute for Defense Analyses

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

[Read IDA's Mission & Values](#)

Research Notes

Spring 2010



Resource Analyses

[download PDF](#)

[view archives](#)

[ABOUT US](#) | [RESEARCH AREAS](#) | [CAREERS](#)

4850 Mark Center Drive, Alexandria, VA 22311 | 703.845.2000

[home](#) | [contact us](#) | [site map](#) | [directions](#) | [facility update](#) | [terms of use](#)

© 2009. All rights reserved.
Web Site Design by New Target

Institute for Defense Analyses
<https://www.ida.org/>

Center for Communications Research - Princeton



805 Bunn Drive
Princeton, New Jersey 08540

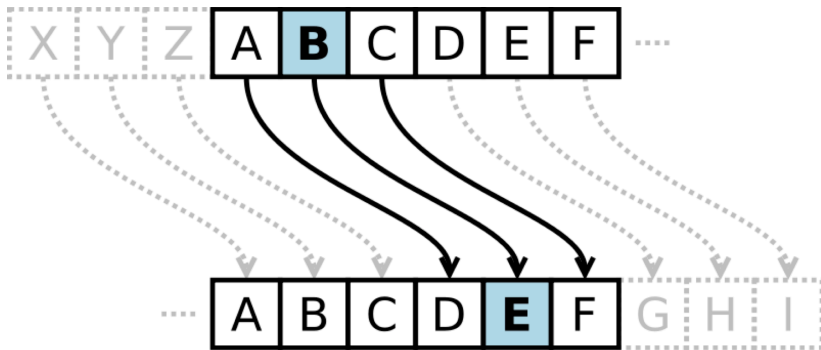
CCR-P is a division of *The Institute for Defense Analyses* in Alexandria, Virginia.

Center for Communications Research in Princeton, NJ
<http://www.idaccr.org/>



Center for Communications Research in La Jolla, CA
<http://www.ccrwest.org/>

What Kind of Mathematics Happens at NSA?



Caesar Cipher

http://en.wikipedia.org/wiki/Caesar_Cipher

ASCII Code Chart

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2		!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL

American Standard Code for Information Interchange

<http://en.wikipedia.org/wiki/ASCII>

Unicode

<http://en.wikipedia.org/wiki/Unicode>

Example of Caesar Cipher

(Local) In[3]:=

```
ShiftCipher[Str_, Shift_Integer] := Module[{lst, n},
  (* Convert input string to a list of Unicode numbers. *)
  lst = ToCharacterCode[Str, "Unicode"];

  (* Determine the number of characters. *)
  n = Length[lst];

  (* Shift by a certain number of places. *)
  newlst = Table[lst[[k]] + Shift, {k, 1, n]];

  (* Return the new string. *)
  Return[FromCharacterCode[newlst]];
];

ShiftCipher["hello", 3]
```

(Local) Out[4]=

khooor

Converting a String to a Number

```
(Local) In[5]:=
StringToNumber[Str_] := Module[{lst, n},
  (*Convert input string to a list of Unicode numbers.*)
  lst = ToCharacterCode[Str, "Unicode"];

  (*Determine the number of characters.*)
  n = Length[lst];

  (*Reconstruct the number written base (2^16).*)
  Return[Sum[lst[[k]] * (2^16)^(k - 1), {k, 1, n}]];
];

StringToNumber["Professor Drasin is Great!"]

(Local) Out[6]=
85 218 816 667 906 701 223 072 976 692 732 706 460 886 071 310 629 547 154 543 158 539 \
502 849 555 798 959 641 179 650 415 408 182 058 457 081 319 952 076 636 240
```

Converting a Number to a String

(Local) In[7]:=

```
NumberToString[Nmbr_Integer] := Module[{n, lst},
  (*Determine the number of "digits" base 2^16. This is the
  number of characters.*)
  n = Ceiling[Log[Nmbr] / Log[2^16]];

  (*Recover list of integers from input.*)
  lst = Table[Mod[Floor[Nmbr / (2^16)^(k-1)], 2^16], {k, 1, n}];

  (*Reconstruct string from the list.*)
  Return[FromCharacterCode[lst, "Unicode"]];
]

NumberToString[
85 218 816 667 906 701 223 072 976 692 732 706 460 886 071 310 629 547 154 543 158 \
539 502 849 555 798 959 641 179 650 415 408 182 058 457 081 319 952 076 636 240]
```

(Local) Out[8]=

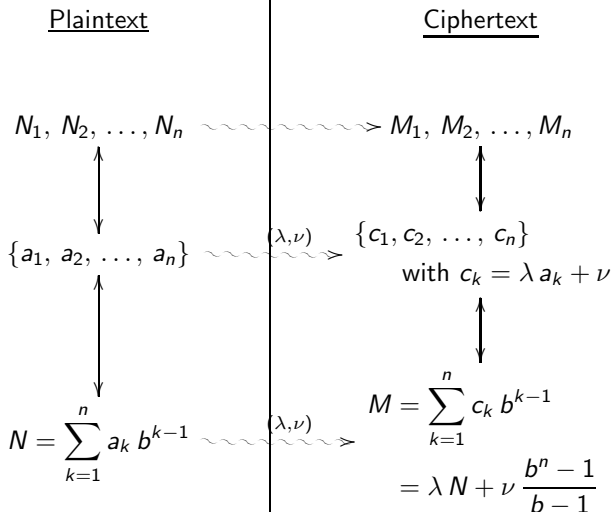
Professor Drasin is Great!



Mathematical Sciences Research Institute Undergraduate Program MSRI-UP 2010

<http://www.msri.org/up/2010/index.html>

Affine Cipher



Solution to Challenge Problem!

BANJO is to **FERNS**
as
PECAN is to **TIGER**

Mathematica Code

```
(Local) In[17]:=
ShiftCipher[Str_, Shift_Integer] := Module[{lst, n},
  (* Convert input string to a list of Unicode numbers. *)
  lst = ToCharacterCode[Str, "Unicode"];

  (* Determine the number of characters. *)
  n = Length[lst];

  (* Shift by a certain number of places. *)
  newlst = Table[lst[[k]] + Shift, {k, 1, n}];

  (* Return the new string. *)
  Return[FromCharacterCode[newlst]];
];

{ShiftCipher["banjo", 4], ShiftCipher["pecan", 4]}

(Local) Out[18]=
{ferns, tiger}
```

Questions?