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

Challenge Problem!

BANJO is to **FERNS**

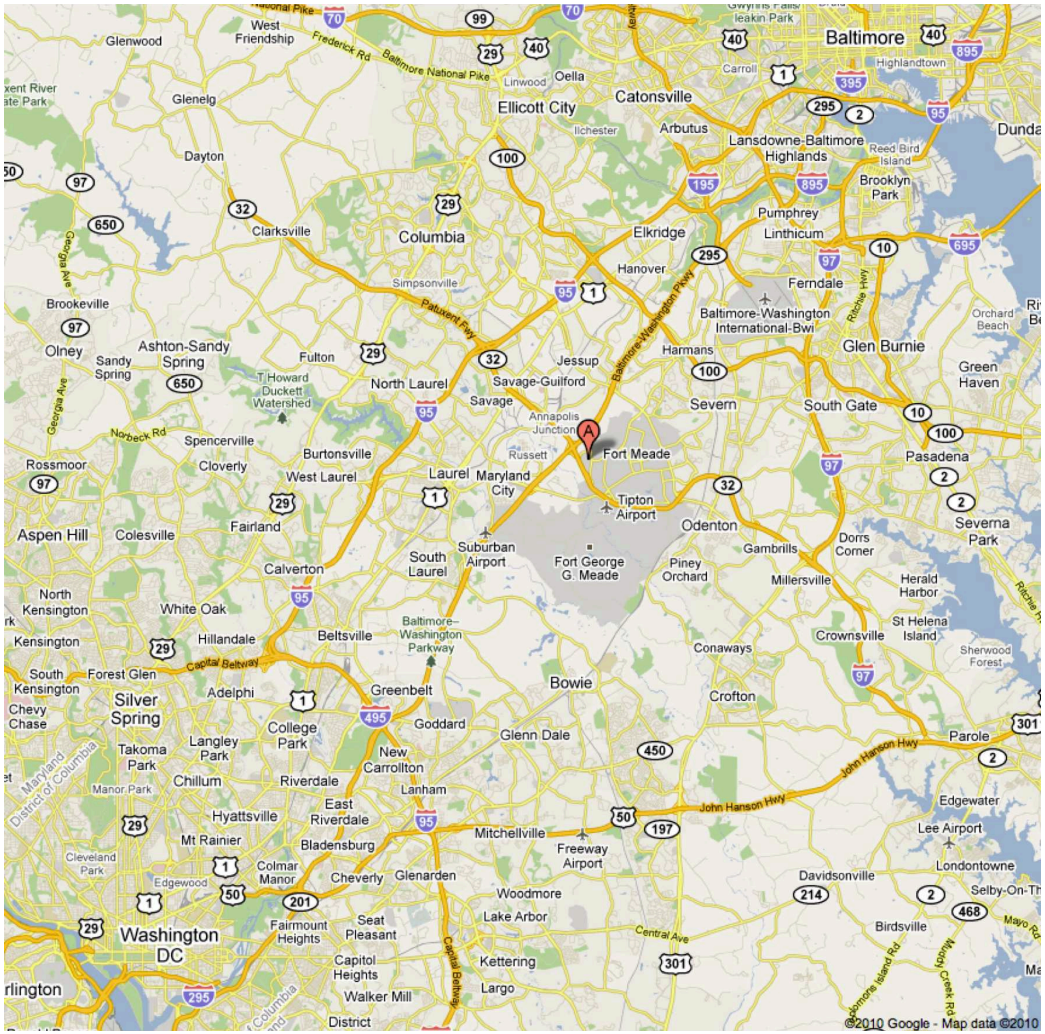
as

PECAN is to **[?]**

Where Are Such Problems Useful?

National Security Agency

http://www.nsa.gov/

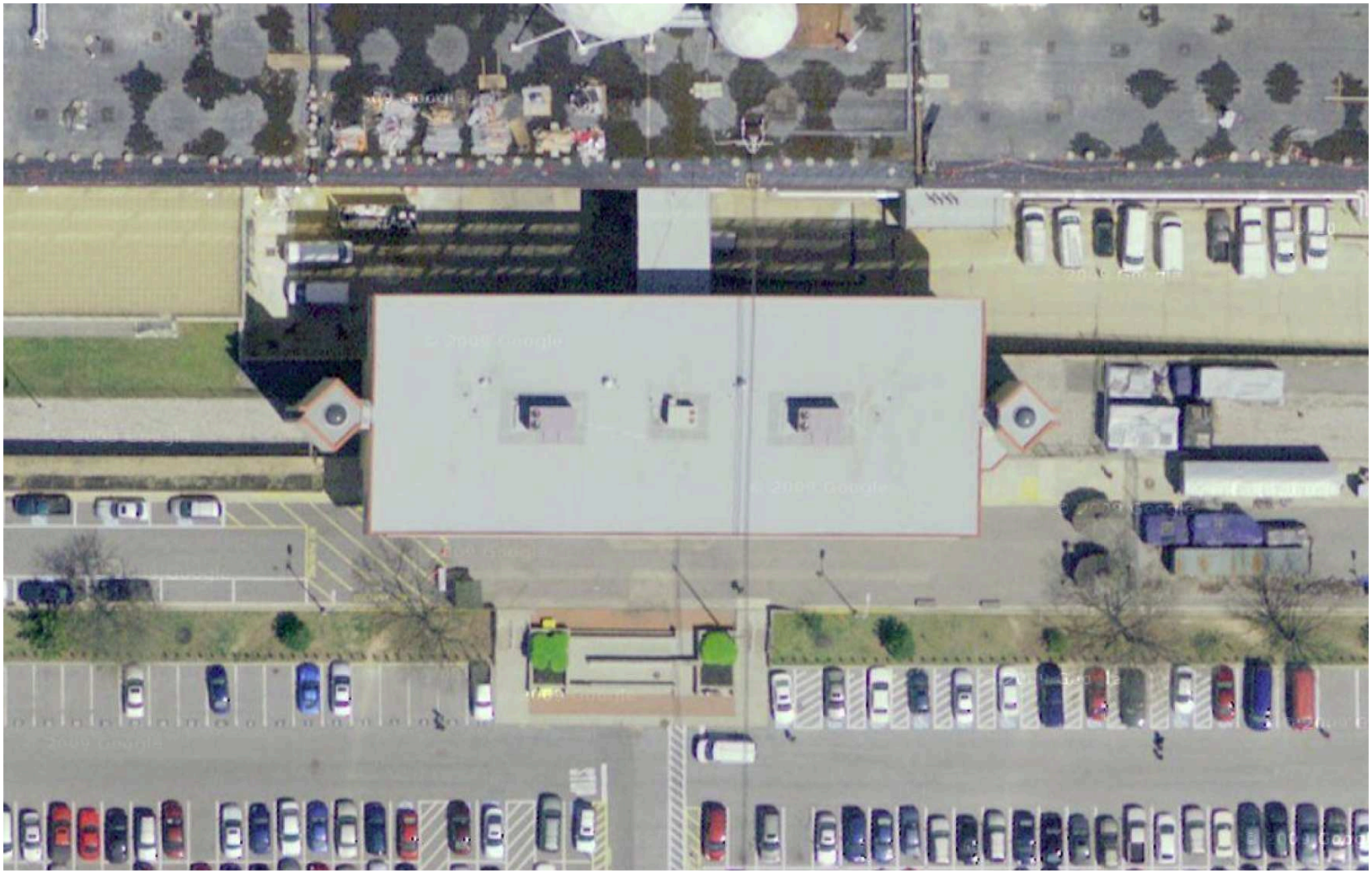


9800 Savage Road, Ft. George G. Meade, MD

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.

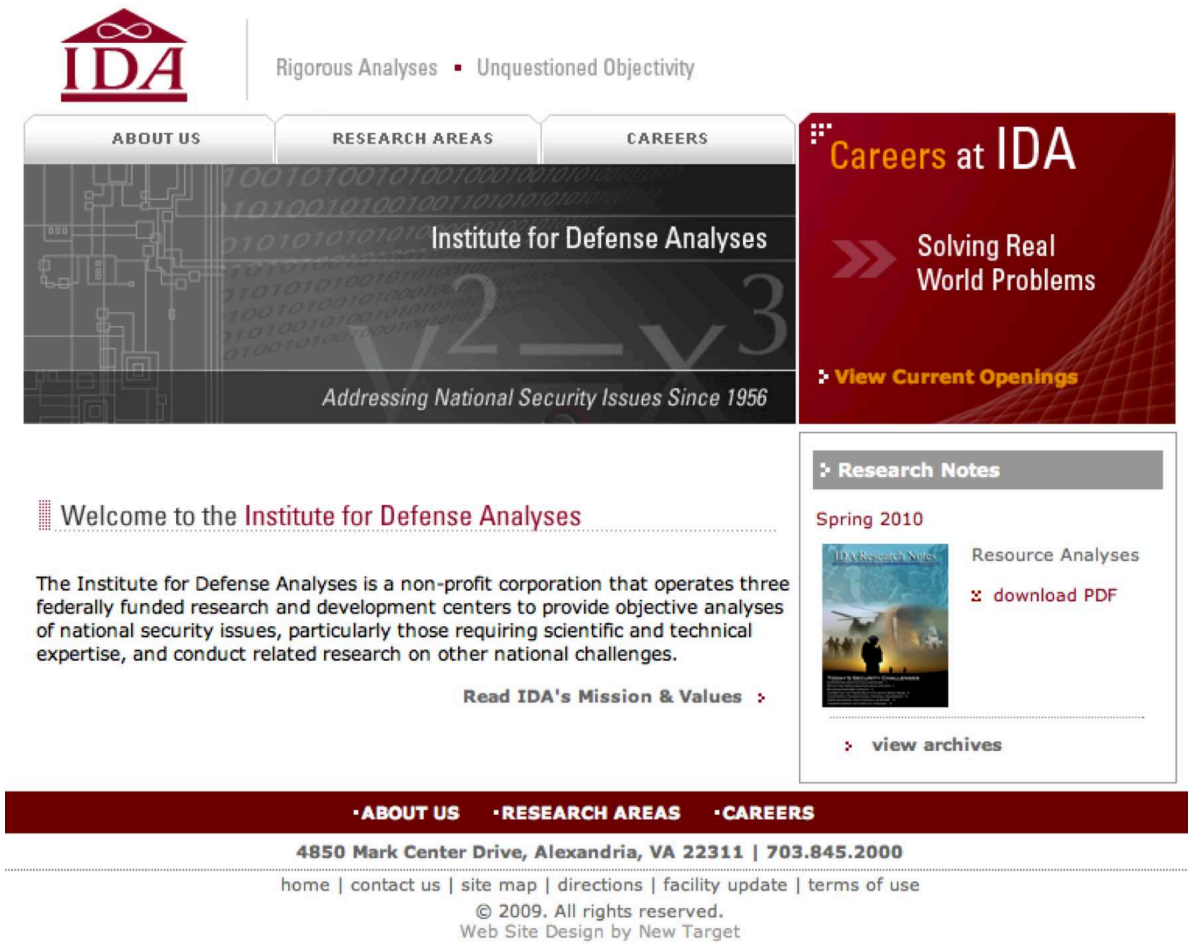
To Work for NSA, Must I Live in Maryland?

Opportunities at NSA

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

Director's Summer Program

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



Institute for Defense Analyses

`https://www.ida.org/`

IDA ***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.

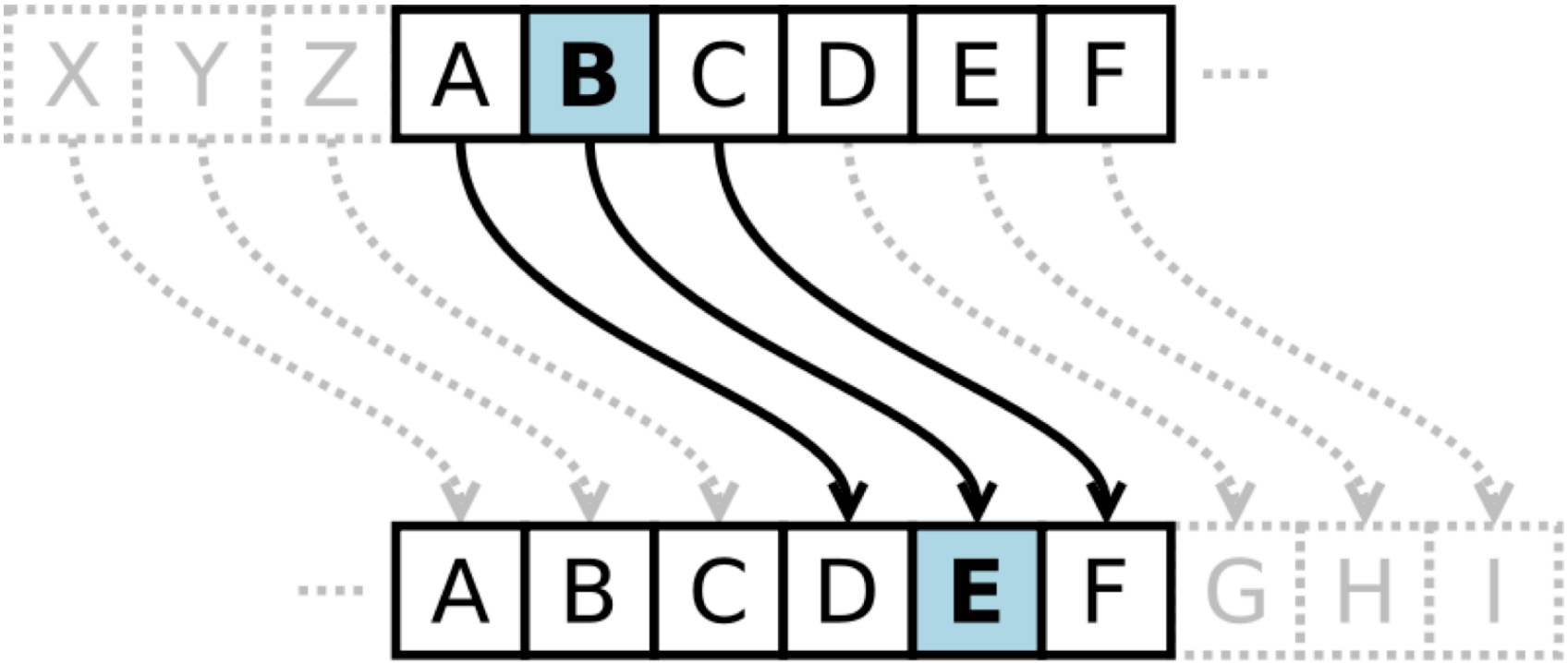
Center for Communications Research in Princeton, NJ
`http://www.idaccr.org/`

Center for Communications Research

La Jolla

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]=

```
khoor
```

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]:=

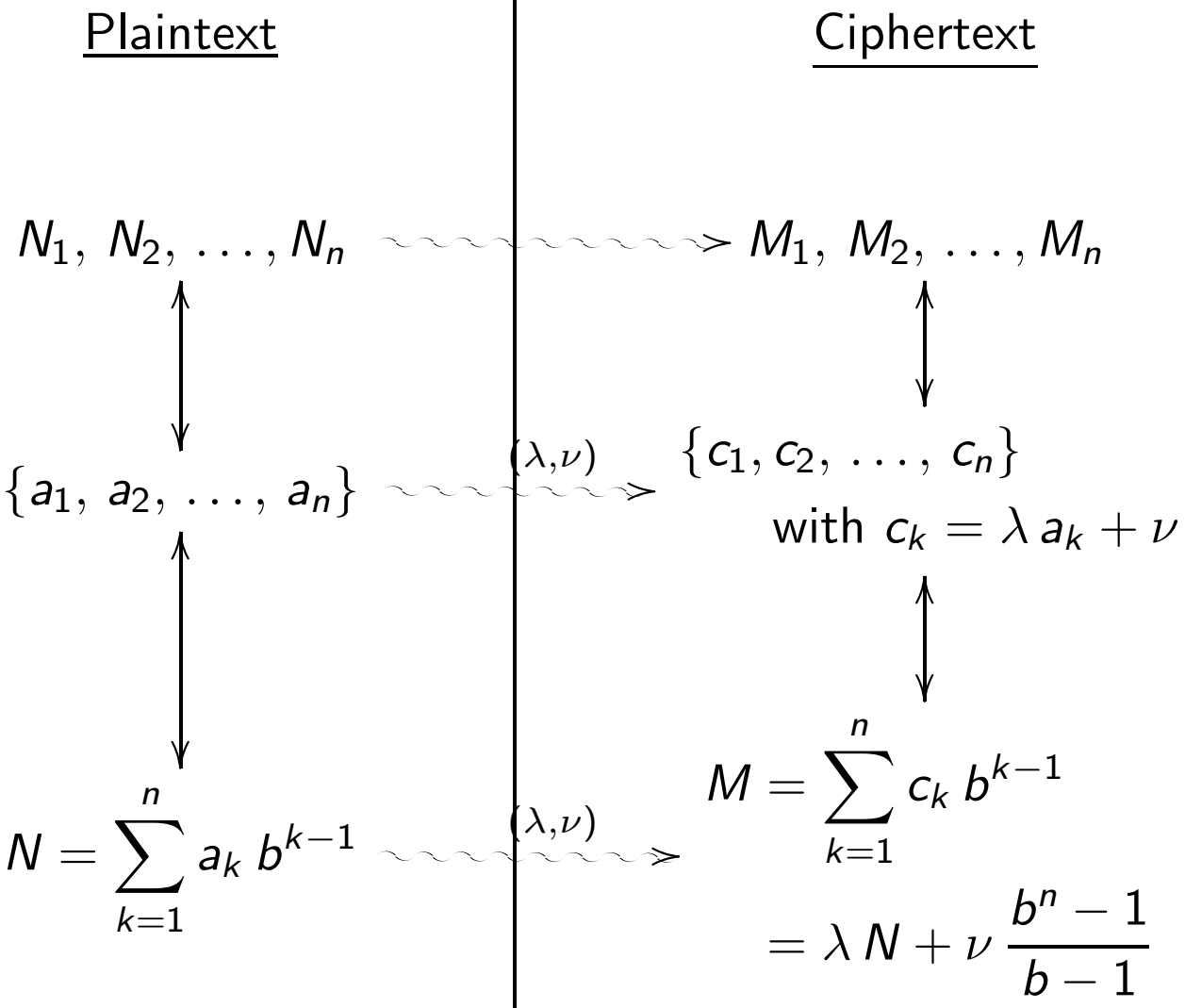
```
NumberToString[Nmbr_Integer] := Module[{n, lst},
  (*Determine the number of "digits" base 2^16. This is the
   number of characters.*)
  n = Ceiling[Log[Nmbr] / Log[2^16]];

  (*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?