Increasing Student Interest in Mathematics using Cryptography

Rick Klima
Appalachian State University
Boone, North Carolina

Neil Sigmon
Radford University
Radford, Virginia

Introductory Concepts

- Cryptography is the science of transmitting information in a secret and confidential manner.

- Applications: Military, Internet transactions, computer data transfer.

What does Cryptography Offer?

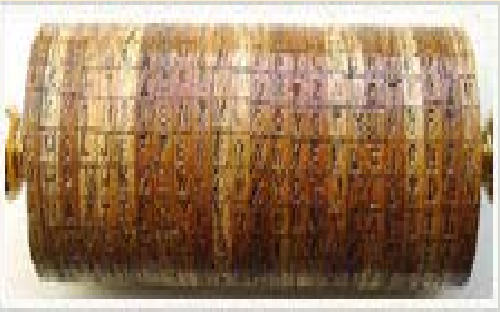
- To execute many cryptographical algorithms, students only need to recall concepts such as division, prime numbers, and basic algebra.

- Cryptography provides an excellent mechanism for increasing student interest in exploring more advanced topics in mathematics.

- Application topics include linear algebra, abstract algebra, number theory, probability, and statistics

Some Famous Cryptographers

- Thomas Jefferson

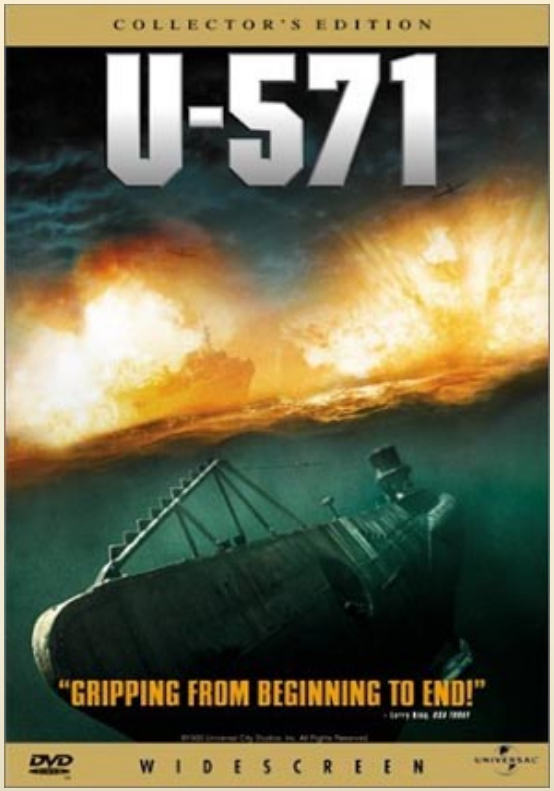


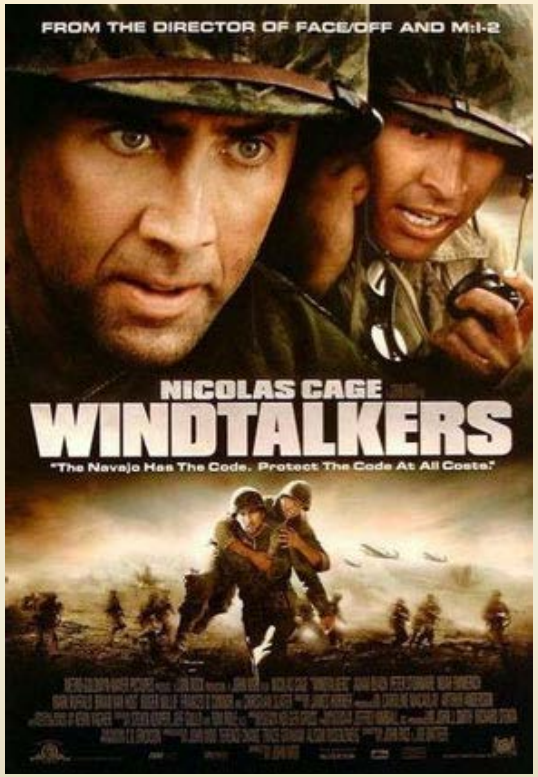
- Edgar Allan Poe

- Navajo Code

Movies


THE
DA VINCI
CODE
05▼19▲06


COLLECTOR'S EDITION
U-571
"GRIPPING FROM BEGINNING TO END!"
DVD
WIDESCREEN


FROM THE DIRECTOR OF FACE/OFF AND M:I-2
NICOLAS CAGE
WINDTALKERS
"The Navajo Has The Code. Protect The Code At All Costs."

Cryptology Course at Radford

- General education course sponsored by the Honors Academy at Radford University.

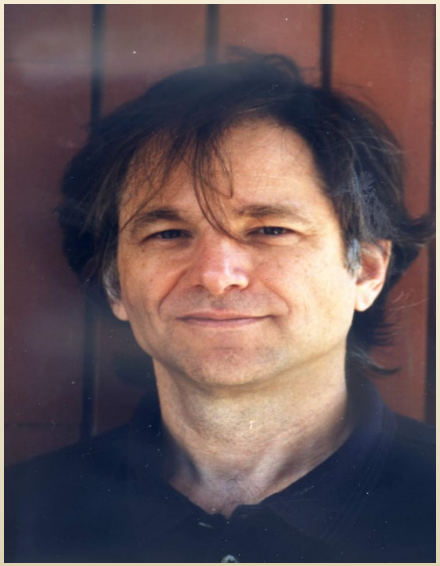
- Course primarily covers classic methods (Caesar, affine, Vigenère, Hill, etc.), historical – Navajo Code, and also delves some into more modern methods – RSA.

The RSA Cryptosystem

- The RSA cryptosystem is named after its developers Ron Rivest, Adi Shamir, and Leonard Adelman.

Ron Rivest

Adi Shamir



Leonard Adelman

RSA Cryptosystem Setup

1. Choose two “large” primes *p* and *q* and compute the quantities

$$m = pq \quad \text{and} \quad \phi(m) = f = (p-1)(q-1).$$

2. A positive integer *e* is chosen where $\gcd(e, f) = 1$. Using the Euclidean algorithm, we calculate an integer *d* where

$$(e \cdot d) \bmod f = 1$$

Note that *d* is the multiplicative inverse of $e \bmod f$, that is $d = e^{-1} \bmod f$. Here, *e* will be called the enciphering exponent (the encryption key) and *d* will be called the deciphering exponent (the decryption key).

3. Using an alphabet assignment to convert from English letters to numbers, compute an English plaintext message number. Assuming that $x < m$, we use the enciphering exponent *e* to encipher the message by computing

$$y = x^e \bmod m$$

Here, *y* will be the “secret” message number (ciphertext) that will be transmitted from the sender to the recipient of the message.

4. To decipher the message, the recipient uses the deciphering exponent *d* to reverse the process of step 3 by computing

$$x = y^d \mod m$$

The alphabet assignment is used to recover the message.

Fact

- When the message number *x* is larger than the modulus *m*, that is, when *x* > *m*, we encipher by breaking *Y* into smaller “block” numbers x_1 , x_2 , … , x_r , and encipher each block separately, that is, we compute

$$y_1 = x_1^e \bmod m \quad , \quad y_2 = x_2^e \bmod m \quad , \ \ldots \ , \quad y_r = x_r^e \bmod m$$

Decipherment is done by computing

$$x_1 = y_1^d \bmod m \quad , \quad x_2 = y_2^d \bmod m \quad , \ \ldots \ , \quad x_r = y_r^d \bmod m$$

Maplets

- Maplets are graphical user interfaces that allows the user to use the power of Maple without using a Maple worksheet.

- Maplets consist of a collection of elements that consist of windows along with their associated layouts, dialogs, and buttons for performing computations.

ASCII Alphabet Assignment

- When converting from letters to numbers the RSA, we will use the ASCII table.

char	code	char	code	char	code	char	code	char	code	char	code
space	32	0	48	@	64	P	80	`	96	p	112
!	33	1	49	A	65	Q	81	a	97	q	113
"	34	2	50	B	66	R	82	b	98	r	114
#	35	3	51	C	67	S	83	c	99	s	115
$	36	4	52	D	68	T	84	d	100	t	116
%	37	5	53	E	69	U	85	e	101	u	117
&	38	6	54	F	70	V	86	f	102	v	118
'	39	7	55	G	71	W	87	g	103	w	119
(	40	8	56	H	72	X	88	h	104	x	120
)	41	9	57	I	73	Y	89	i	105	y	121
*	42	:	58	J	74	Z	90	j	106	z	122
+	43	;	59	K	75	[	91	k	107	{	123
,	44	<	60	L	76	\	92	l	108	|	124
-	45	=	61	M	77	]	93	m	109	}	125
.	46	>	62	N	78	^	94	n	110	~	126
/	47	?	63	O	79	_	95	o	111	del	127

Example

- Suppose the receiver of a message creates a public key with the RSA parameter Maple using the numbers

  54242452544 and 43245424542

  to create two prime numbers and chooses e = 134137 as the enciphering exponent.

The receiver makes the parameters

m = 2345737889838909867283 and e = 134137 public

The receiver keeps the following parameters secret

p = 54242452567,

q = 43245424549,

f = 2345737889741421990168

d = 3400119414497302590 25

Using the RSA encryption Maplet, the sender takes the receivers public key

m = 2345737889838909867283 and e = 134137

to encrypt the following message:

Maplets make it easy to create a public key and to quickly encipher and decipher messages using RSA algorithm!

Hence, the ciphertext is:

[630745417108630048747, 188213546991813469268 1, 226699317000694577674, 231994643327381373128 1, 1822471318437511634736,139890296517155141910 0, 172976180604271241953 3, 267890942674449986 2, 1144532595277961741049,206979904265153719711 0, 376200266194991291452, 487065980145284287303, 707623905885910184189, 3587549465990997048 6]

To decipher the message, the receiver uses the RSA decryption Maplet with the parameters

m = 234573788983890986728 3

d = 340011941449730259025

Security of the RSA Cryptosystem

1. The security of the method is based on keeping the deciphering exponent *d* secret. To keep *d* secret, the primes *p* and *q* must be kept secret. If *p* and *q* can be secret, $f = (p-1)(q-1)$ can be kept secret and $d \equiv e^{-1} \pmod{f}$ cannot be computed.

2. However, it is much easier to find primes *p* and *q* and form $m = pq$ then it is to start with *m* and factor as $m = pq$.

Example

Suppose a sender uses the public key

m = 2345737889838909867283 and e = 134137

to encrypt the message

[19413358548180397864 49, 726058883450368663 34,
142264599177508481 6137, 177915729933357468 3296,
153978253148856399 4152, 229239869952117027 4407,
190212809558355058 5001, 212464764218259022 1928,
170613752144048711 2136, 133743582514448409 8480,
989503397947861977 542, 191492729912214276 9468,
721974133877527925 763, 138951569532113920 3177,
272122896369346617 929, 124370633257950402 4901,
682902026985031049 178, 162372190476429531 4626,
127126258460332603 452, 784232821658527375 64,
188771920535555258 7446, 758571389653163238 443,
134621249994950830 8898, 147573721908999980 7863,
257018094864891631 356, 181799832780872206 4884,
207729621680910807 3870, 405288827971040729 437]

Using the RSA breaker Maplet, m factors into the primes

$$p = 43245424549 \text{ and } q = 54242452567$$

and the message deciphers as

"If the size of the primes used to form the encryption modulus are not large enough, the RSA system can be broken easily by factoring. In practice, prime of 100 digits or more are used to create more secure RSA schemes."

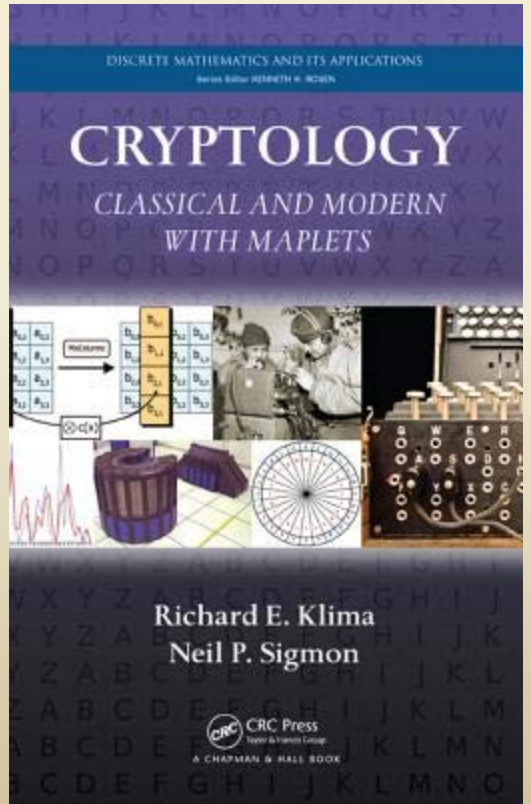
Other Schools Offering Cryptography

- High schools that have offered a similar course to Radford's cryptography course include the Southwest Virginia Governor's School and Appalachian Summer Regional Governor's School.

- These schools are designed to offer high school students special educational opportunities, including earning college credit.

Reference

- Klima, Richard E. and Sigmon, Neil P. *Cryptology: Classical and Modern with Maplets*, CRC Press, 2012.



Contact Information

- Rick Klima: klimare@appstate.edu
  Department of Mathematical Sciences
  Appalachian State University
  Boone, North Carolina 28608

- Neil Sigmon: npsigmon@radford.edu
  Department of Mathematics and Statistics
  Radford University
  Radford, Virginia 24142