

# Classical Number Theory and Modern Cryptography

Keith Jones  
Binghamton University

February 2010

## Table 1: The Caesar Cipher

Original:	A	B	C	D	E	F	G	H	I	J	K	L	M
Shift 3:	D	E	F	G	H	I	J	K	L	M	N	O	P

Original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shift 3:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

## Table 2: A Monoalphabetic Substitution Cipher

Original:	A	B	C	D	E	F	G	H	I	J	K	L	M
Shuffled:	E	K	G	U	J	L	V	C	X	T	Y	N	H

Original	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shuffled:	F	Z	B	S	A	O	D	P	Q	R	M	I	W

# A Sample Cryptogram

A cryptogram on the beauty of cryptograms...

                              
"L N W    O R    R U    L N I H    K X N K    X H

                            
Q N W    U W V B    S O W I    E H V N P N K O U W

                           
S E U L    U W H    G O W I    U S    V N A U E

                         
A B    K N G O W J    M F    N W U K X H E."

—                   
— N W N K U V H    S E N W Q H

Hints and solution available at: <http://www.math.binghamton.edu/grads/kjones/cryptograms>

## Table 3: Conversion to Digits

A	=	00	N	=	13
B	=	01	O	=	14
C	=	02	P	=	15
D	=	03	Q	=	16
E	=	04	R	=	17
F	=	05	S	=	18
G	=	06	T	=	19
H	=	07	U	=	20
I	=	08	V	=	21
J	=	09	W	=	22
K	=	10	X	=	23
L	=	11	Y	=	24
M	=	12	Z	=	25
<i>and</i> space = 99					

# RSA Example

1. Let  $p = 97$  and  $q = 101$ .

# RSA Example

1. Let  $p = 97$  and  $q = 101$ .

Then  $n = pq = 9797$  and  $\phi(n) = (p - 1)(q - 1) = 9600$ .

# RSA Example

1. Let  $p = 97$  and  $q = 101$ .

Then  $n = pq = 9797$  and  $\phi(n) = (p - 1)(q - 1) = 9600$ .

2. Choose  $k = 23$  and  $j = 2087$ . One can verify that  $k$  and  $\phi(n)$  are relatively prime, and that  $kj \equiv 1 \pmod{\phi(n)}$ .

# RSA Example

1. Let  $p = 97$  and  $q = 101$ .

Then  $n = pq = 9797$  and  $\phi(n) = (p - 1)(q - 1) = 9600$ .

2. Choose  $k = 23$  and  $j = 2087$ . One can verify that  $k$  and  $\phi(n)$  are relatively prime, and that  $kj \equiv 1 \pmod{\phi(n)}$ .

3. We will encrypt the message **HELLO**. We will encode letters using the previously described mechanism:  $A \mapsto 00$ ,  $B \mapsto 01$ , etc.

RSA Example, continued. ( $n = 9797$ ,  $k = 23$ ,  $j = 2087$ )

$H \mapsto 07$

$E \mapsto 04$

$L \mapsto 11$

$L \mapsto 11$ , again

$O \mapsto 14$

So HELLO becomes 0704111114.

RSA Example, continued. ( $n = 9797$ ,  $k = 23$ ,  $j = 2087$ )

$H \mapsto 07$

$E \mapsto 04$

$L \mapsto 11$

$L \mapsto 11$ , again

$O \mapsto 14$

So HELLO becomes 0704111114.

We will use blocks of length  $3^\dagger$ . Since we have 10 digits, we'll add a space (99).

$M = 070411111499 \mapsto 070\ 411\ 111\ 499$ .

$\dagger$  Note this technically isn't small enough to guarantee that each block will be relatively prime to  $n$ .

# RSA Example, continued. ( $n = 9797$ , $k = 23$ , $j = 2087$ )

$$070 \mapsto 70^{23} \pmod{9797} \mapsto 7002$$

$$411 \mapsto 411^{23} \pmod{9797} \mapsto 8208$$

$$111 \mapsto 111^{23} \pmod{9797} \mapsto 4131$$

$$499 \mapsto 499^{23} \pmod{9797} \mapsto 4228$$

## RSA Example, continued. ( $n = 9797$ , $k = 23$ , $j = 2087$ )

$$070 \mapsto 70^{23} \pmod{9797} \mapsto 7002$$

$$411 \mapsto 411^{23} \pmod{9797} \mapsto 8208$$

$$111 \mapsto 111^{23} \pmod{9797} \mapsto 4131$$

$$499 \mapsto 499^{23} \pmod{9797} \mapsto 4228$$

Cipher: 7002 8208 4131 4228

# RSA Example, continued. ( $n = 9797$ , $k = 23$ , $j = 2087$ )

$$070 \mapsto 70^{23} \pmod{9797} \mapsto 7002$$

$$411 \mapsto 411^{23} \pmod{9797} \mapsto 8208$$

$$111 \mapsto 111^{23} \pmod{9797} \mapsto 4131$$

$$499 \mapsto 499^{23} \pmod{9797} \mapsto 4228$$

Cipher: 7002 8208 4131 4228

$$7002 \mapsto 7002^{2087} \pmod{9797} \mapsto 070$$

$$8208 \mapsto 8208^{2087} \pmod{9797} \mapsto 411$$

$$4131 \mapsto 4131^{2087} \pmod{9797} \mapsto 111$$

$$4228 \mapsto 4228^{2087} \pmod{9797} \mapsto 499$$

## References and Further Reading

- ▶ Elementary Number Theory, *David M. Burton*
- ▶ The Art of Proof, *Matthias Beck & Ross Geoghegan*
  - ▶ free at <http://math.sfsu.edu/beck/aop.html>
  - ▶ Appendix B on Diffie-Hellman
- ▶ The (simple) mathematics of RSA. *Martin Ouwehand*.
  - ▶ Essay at <http://certauth.epfl.ch/rsa/>
- ▶ Disquisitiones Arithmeticae. *Carl Friedrich Gauss*.
  - ▶ Available at Google Books.
- ▶ ...and of course WIKIPEDIA