CRYPTOGRAPHY AND PRIME NUMBERS

DAN CIUBOTARU

1. Substitution ciphers

The following text is encoded using a straight substitution cipher:

NOT NUA JMPETZ UTST ZENNELV EL NOT JEGELV SAAW, UMENELV

KAS NOTES OAZNTZZ, UOA UMZ ZJEVONJX PTJMXTP. NOT PMCVONTS

AK NOT KMWEJX UMZ UENO NOTW, AL NOT NOTASX NOMN ZOT UACJP

QTTY NOT GEZENASZ ADDCYETP PCSELV NOT UMEN.

NOT DOEJP UMZ YTSOMYZ ZEI XTMSZ AJP, ZLCR LAZTP, KSTDQTJP,

RCDQ NAANOTP MLP RTZYTDNMDJTP. ZOT WMELNMELTP M PTTY

ZEJTLDT MLP NOT NUA JMPETZ YTTSTP PACRNKCJJX MN OTS.

KELMJJX, ALT AK NOTW WCNNTSTP NA NOT ANOTS, “LAN GTSX

Y-S-T-N-N-X, E KTMS,” DMSTKCJJX ZYTJJELV NOT QTX UASP.

UOTSTCYAL NOT DOEJP YEYTP CY, “RCN MUKCJ Z-W-M-S-N!”

Below there are the character frequencies for this text. The letters B, F, H do not appear.

A	C	D	E	G	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	14	10	28	3	1	23	10	18	25	44	31	24	4	5	22	60	14	7	7	11	13	23

2. Modular arithmetic and prime numbers

1. A number a has an inverse modulo n if and only if $\gcd(a, n) = 1$.

2. (Fermat's little theorem) If p is a prime number, and a is an integer such that $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

3. Which numbers a, $1 \leq a < p$ have the property that

$$a^2 \equiv 1 \pmod{p},$$

is p is a prime.

3. (Wilson's theorem) If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

4. (Euler's ϕ-function) For every positive integer n, define the value of the function $\phi(n)$ to be the number of $1 \leq k \leq n$, such that $\gcd(n, k) = 1$.

(a) $\phi(p) = p - 1$ if and only if p is prime.
(b) If $\gcd(n, m) = 1$, then $\phi(nm) = \phi(n)\phi(m)$.
(c) Using the factorization of n into primes (i.e., the Fundamental Theorem of Arithmetic), find a formula for $\phi(n)$.

4. (Extension of Fermat's little theorem) If $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

5. Let p, q be two numbers (not necessarily prime) such that $\gcd(p, q) = 1$. If $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, then $a \equiv b \pmod{pq}$.

1. Compute 2^{12} mod 10.

2. Compute 2^{24} mod 10.

3. Compute 2^{103} mod 10.

4. Compute 5^{103} mod 103.

5. Compute 10^{103} mod 103.

6. Compute 2^{561} mod 561.

7. Compute 3^{561} mod 561.

8. Compute 6^{41} mod 55.

References

[1] Tom Davis, *Cryptography*
[2] Tom Davis, *RSA encryption*
[3] Peter Trapa, *Introduction to primes*

(D. Ciubotaru) Dept. of Mathematics, University of Utah, Salt Lake City, UT 84112
E-mail address: `ciubo@math.utah.edu`