Cryptography

David Malone

7 March 2018

Cryptography

Cryptography is the study of sending secret messages.
Often combined with cryptanalysis — how to break these systems.

Two different ways:

1. They are both mathematical subjects.
2. Many nice ideas.
3. There are many classical ciphers that are easy to teach.
4. Some modern cryptography is complicated, but built on easier ideas.

Encrypting data

Caesar Cipher:

$$\texttt{Hello World} \rightarrow \texttt{Lipps Asvph}$$

Key is d.

Treat letters as numbers and practicce clock (modular) arithmetic:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

If m is the number for a letter of the message then $f(m)$ is what we get when we encrypt.

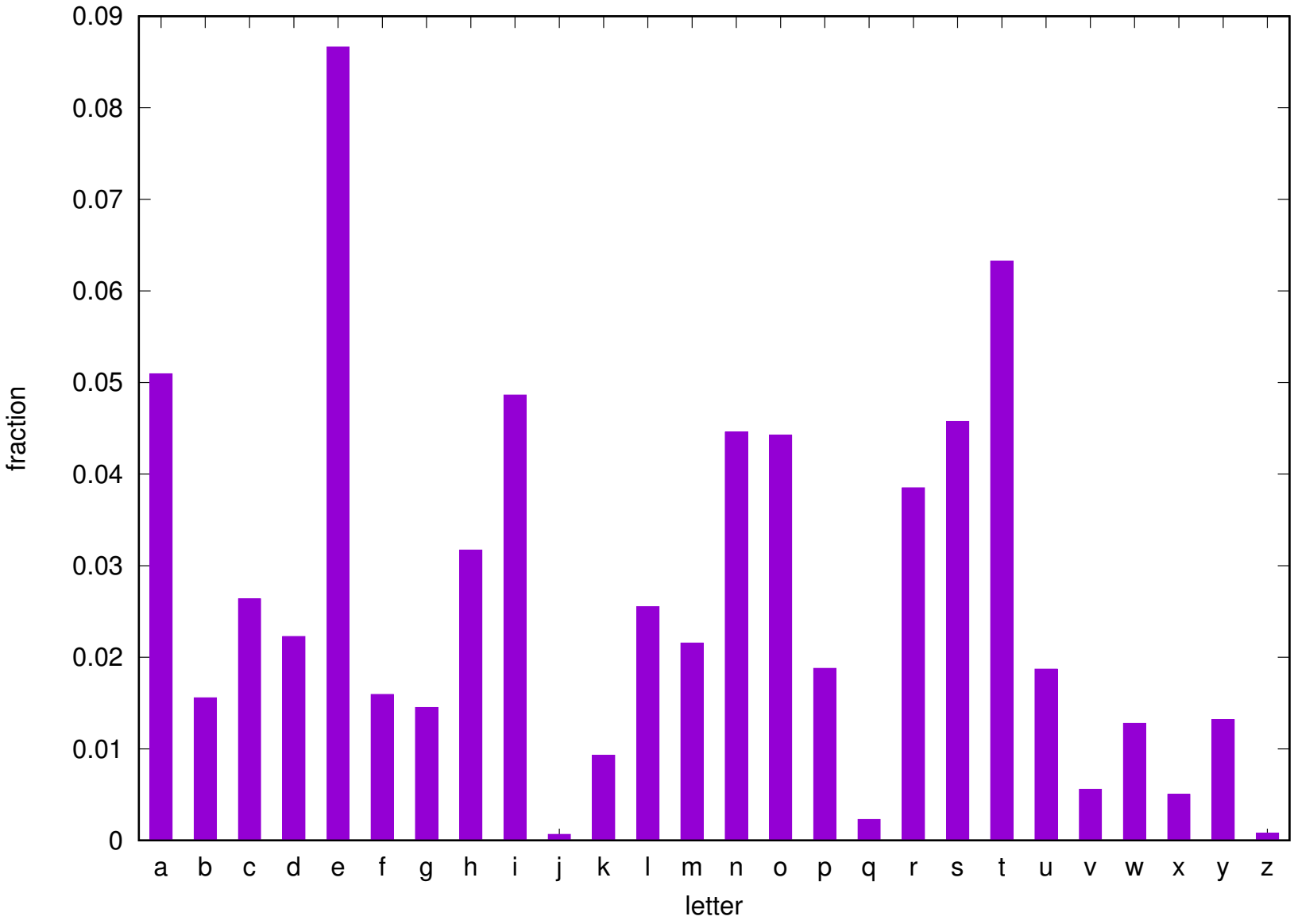
Brute Force Attacks

0	Wklv	lv	d	vhfuhw	phvvdjh	13	Jxyi	yi	q	iushuj	cuiiqwu
1	Xlmw	mw	e	wigvix	qiwweki	14	Kyzj	zj	r	jvtivk	dvjjrxv
2	Ymnx	nx	f	xjhwjy	rjxxflj	15	Lzak	ak	s	kwujwl	ewkksyw
3	Znoy	oy	g	ykixkz	skyygmk	16	Mabl	bl	t	lxvkxm	fxlltzx
4	Aopz	pz	h	zljyla	tlzzhnl	17	Nbcm	cm	u	mywlyn	gymmuay
5	Bpqa	qa	i	amkzmb	umaaiom	18	Ocdn	dn	v	nzxmzo	hznnvbz
6	Cqrb	rb	j	bnlanc	vnbbjpn	19	Pdeo	eo	w	oaynap	iaoowca
7	Drsc	sc	k	combod	wocckqo	20	Qefp	fp	x	pbzobq	jbppxdb
8	Estd	td	l	dpncpe	xpddlrp	21	Rfgq	gq	y	qcapcr	kcqqyec
9	Ftue	ue	m	eqodqf	yqeemsq	22	Sghr	hr	z	rdbqds	ldrrzfd
10	Guvf	vf	n	frperg	zrffntr	**23**	This	is	a	secret	message
11	Hvwg	wg	o	gsqfsh	asggous	24	Uijt	jt	b	tfdsfu	nfttbhf
12	Iwxh	xh	p	htrgti	bthhpvt	25	Vjku	ku	c	ugetgv	oguucig

Functions can be Complicated

Us tw, so dsu us tw- ugyu hi ugw pxwiuhsd:
Vgwugwo ’uhi dstlwo hd ugw zhde us ixqqwo
Ugw ilhdfi yde yoosvi sq sxuoyfwsxi qsouxdw
So us uykw yozi yfyhdiu y iwy sq uosxtlwi,
Yde tn saasihdf wde ugwz. Us ehw- us ilwwa-
Ds zsow; yde tn y ilwwa us iyn vw wde
Ugw gwyouyrgw, yde ugw ugsxiyde dyuxoyl igsrki
Ugyu qlwig hi gwho us. ’Uhi y rsdixzzyuhsd
Ewcsxuln us tw vhig’e. Us ehw- us ilwwa.
Us ilwwa- aworgydrw us eowyz: yn, ugwow’i ugw oxt!

Using Statistics



To me, or iot to me- tsht na tse kdeatnoi:
Bsetser ’tna iomuer ni tse ynil to adccer
Tse aunipa hil hrroba oc odtrhpeoda cortdie
Or to thve hrya hphniat h aeh oc trodmuea,
Hil mg owwoanip eil tsey. To lne- to aueew-
Io yore; hil mg h aueew to ahg be eil
Tse sehrthfse, hil tse tsodahil ihtdrhu asofva
Tsht cueas na senr to. ’Tna h foiadyyhtnoi
Lejodtug to me bnas’l. To lne- to aueew.
To aueew- werfshife to lrehy: hg, tsere’a tse rdm!

Conclusion

1. Cryptography uses several mathematical areas:
   - Numbers,
   - Functions,
   - Stats,
   - Probability (theory of secrecy!),
   - Number theory.
2. Handy activities to keep people busy.
3. Links in with history and technology nicely.