

Decimation

Linguistics 484

Shift ciphers

- * There are 25 shift ciphers
- * All can be broken by recognizing pattern of standard alphabet
- * Can also be solved by method of exhaustion

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Decimation

- * Shift ciphers use $a = b + k$ (with wraparound)
- * If $k = 16$ and $b = 'A'$ (letter 1) then a is $1 + 16 = 17$, which is $'Q'$
- * What if we use $a = b * k$ (with wraparound)

A	B	C	D	E	F	G	H	I	J	K	L	M
5	10	15	20	25	30	35	40	45	50	55	60	65
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
70	75	80	85	90	95	100	105	110	115	120	125	130

$$a = b * 5$$

A	B	C	D	E	F	G	H	I	J	K	L	M
5	10	15	20	25	4	9	14	19	24	3	8	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
18	23	2	7	12	17	22	1	6	11	16	21	26

$$a = b * 5 \text{ mod } 26$$

Modular arithmetic

- * Integer arithmetic with wraparound is called modular arithmetic. It turns up all over the place.
- * As the alphabet is 26 characters, we are especially interested in arithmetic modulo 26
- * We call 26 the modulus

Remainders and residues

- * Given a number $a > 25$, we can write it as $a = k * 26 + b$, where k is a non-negative integer (i.e. $0, 1, 2, \dots$)
- * b is called the residue of a modulo 26
- * In modular arithmetic, we treat numbers with the same b as equivalent.

Encoding

- * Simply fill in the table as before.

A	B	C	D	E	F	G	H	I	J	K	L	M
E	J	O	T	Y	D	I	N	S	X	C	H	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	W	B	G	L	Q	v	A	F	K	P	W	Z

$$a = b * 5 \pmod{26}$$

Inverses?

- * Shifts obviously have inverses, for example $19+7 \bmod 26 = 0$
- * But is there a solution to $x*5 = 1 \bmod 26$? If so, can use it for decoding
- * Yes. $21*5=105=(4*26)+1$

Decoding

* So there is an inverse.

A	B	C	D	E	F	G	H	I	J	K	L	M
21	42	63	84	105	126	147	168	189	210	231	252	273
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
294	315	336	357	378	399	420	441	462	483	504	525	546

$$a = b * 21 \text{ mod } 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M
21	42	63	84	105	126	147	168	189	210	231	252	273
21	16	11	6	1	22	17	12	7	2	23	18	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
294	315	336	357	378	399	420	441	462	483	504	525	546
8	3	24	19	14	9	4	25	20	15	10	5	26

$$a = b * 21 \text{ mod } 26$$

Modular arithmetic

- * What happens if you choose to multiply by 2?

A	B	C	D	E	F	G	H	I	J	K	L	M
2	4	6	8	10	12	14	16	18	20	22	24	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	4	6	8	10	12	14	16	18	20	22	24	26

$$a = 2 * b \text{ mod } 26$$

This is no good

- * The problem is that 2 and 26 share factors, so the output alphabet doesn't cover the whole of the input alphabet.
- * Thus, we can't possibly have an inverse.

Inclass

TFHSH	SKEMA	HSEVR	QYSHM	CUKEQ	NMRHT	GNMSH	STSNB
KHTTK	RRKSR	TFEMT	FRSRE	SEMAE	MAHSE	DNUTT	FQRRL
HKRSK	NMCHT	SDQRE	ATFET	MNONH	MTRXG	RRASE	PUEQT
RQNBE	LHKRH	THSSR	OEQET	RABQN	LTFRL	EHMKE	MADYE
SGEQG	RKYOR	QGROT	HDKRG	QRRJN	NZHMC	HTSWE	YTFQN
UCFEW	HKARQ	MRSSN	BQARR	SEMAS	KHLRE	BEVNQ	HTRQR
SNQTN	BTFRL	EQSFF	RMTFR	VRCRT	ETHNM	ESLHC	FTDRS
UOONS	RAHSS	GEMTN	QETKR	ESTAW	EQBHS	FMNTQ	RRSNB
EMYLE	CMHTU	AREQR	TNDRS	RRMMR	EQTFR	WRSTR	QMRXT
QRLHT	YWFRQ	RBNQT	LNUKT	QHRST	EMASE	MAWFR	QREQR
SNLRL	HSRQE	DKRBQ	ELRDU	HKAHM	CSTRM	EMTRA	AUQHM
CSULL	RQDYT	FRBUC	HTHVR	SBQNL	GFEQK	RSTNM	AUSTE
MABRV	RQLEY	DRBNU	MAHMA	RRATF	RDQHS	TKYOE	KLRTT
NDUTT	FRWFN	KRHSK	EMAWH	TFTFR	RXGRO	THNMN	BTFHS
WRSTR	QMONH	MTEMA	EKHMR	NBFEQ	AWFHT	RDREG	FNMTF
RSREG	NESTH	SGNVR	QRAWH	TFEAR	MSRUM	ARQCQ	NWTFN
BTFRS	WRRTL	YQTKR					

Homework 2

QCTAD	OPQMO	LATPP	LODPS	VVSPD	KSUTO	YHSOB	TOLLJ
VDQCA	LOQYM	RMDHP	SWLRQ	CDJSA	QTOPS	HRQSQ	DLKLW
PTOUD	KBJTQ	LHLLG	TSOKT	PQHYP	MLKSA	OSJTV	CDICQ
LLGRM	QCTBO	TSQTP	QMSOQ	LAWLQ	CQCTH	TKBQC	SKFWO
TSFQC	LAQCT	OLLJC	TPSDF	MTOCS	MPDJD	BCQVL	KFTOQ
LPTTC	DJTJM	HLYTF	DKSMO	LETIQ	ALODJ	MOLUD	KBPMT
IRHSQ	DUTGK	LVHTF	BTWYM	OSIQD	ISHSK	FJTIC	SKDIS
HLMTO	SQDLK	PWRQQ	CTVLO	HFVLR	HFPLL	KWTPT	KPDWH
TLADQ	PRPTA	RHKTP	PSKFC	TAHSQ	QTOTF	CDJPT	HAQCS
QSJLO	TKLWH	TTXSH	QTFQC	LRBCQ	KTUTO	PMOSK	BDKSK
YLQCT	OJSKP	CTSFT	UTOYL	KTGKT	VCLVH	SWLOD	LRPQC
TRPRS	HJTQC	LFDPL	ASQQS	DKDKB	QLSOQ	PSKFP	IDTKI
TPVCT	OTSPW	YCDPI	LKQOD	USKIT	QCTJL	PQDBK	LOSKQ
MTOPL	KSQSO	TSPLK	SWHTI	CSOBT	SKFVD	QCSDH	QQHTW
LFDHY	HSWLR	OJDBC	QVODQ	TWLLG	PDKMC	DHLPL	MCYML
TQOYM	LHDQD	IPHSV	PJSQC	TJSQD	IPSKF	QCTLH	LBVVD
QCLRQ	QCTHT	SPQSP	PDPQS	KITAO	LJBTK	DRPLO	PQRFY