

Chapter 2

Substitution Ciphers

2.1 Keyword Substitution Ciphers

1. (a) VZUWS WSD AXGDR RDGDAOUAD
(b) X BDH HUAMF UR FDKADW HAEWERP
(c) THE FALL OF THE HOUSE OF USHER
3. (a) G TGJN OB G BGTNBUJ TREP
(b) AGWM WNJJS PJGYNA KGRY GMM
(c) ALAN HALE JR. PLAYED THE SKIPPER.
5. (a) DMKIZAMN GWREK WG AYARC UWKN
(b) MHMGAM BXMFC LXMNCA HWDD FWKKN
(c) KEN CURTIS PLAYED FESTUS HAGGEN.

2.2 A Maplet for Substitution Ciphers

1. (a) KSELMADR XAD BUA JDUJLD HSU KXRRUW SXGD MUPF
(b) KSXFERP IUZA WXEL URLI PDWF IUZ QXKC HSDAD IUZ FWXAWDM
(c) A GOOD MAN IS HARD TO FIND, BUT FINDING A GOOD DOG IS EASY.
3. (a) TQ TG RSH FJUGRATGQ TG PJJGH GJORS LAOJDTGA
(b) TQ AR AG HDHVARTJG JI FJOH RSAG RSOHH RSJUQAGC IHHR
(c) HAS WON THREE FCS NATIONAL CHAMPIONSHIPS IN FOOTBALL
5. (a) LGF EFRLVFN RIO LGF XWVVUIC NLWIFN RXF TRBWYN XWQH ERION
(b) LGF MGW RIO VFO PFAAFVUI RXF RVNW DFXS MFVV HIWMI ERION
(c) THE DOOBIE BROTHERS AND SKYNYRD ARE PRETTY GOOD TOO.
7. COJSHOIOJWOHHAORTLLORRBTHSDERYOVQEYKTLVJBKLTRKJSDQOOSDEJCRVJNSDQOOSDEJCRK
JHYKYTBVIEHYKYTQQOHECEKJVJNSDOCQOOJAVYMLGOQR

2.3 Cryptanalysis of Substitution Ciphers

1. (a) The cipher is a simple keyword substitution cipher with the keywords THE NEW DEAL. The plaintext is THE TEST OF OUR PROGRESS IS NOT WHETHER WE ADD TO THE ABUNDANCE OF THOSE WHO HAVE MUCH. IT IS WHETHER WE PROVIDE ENOUGH TO THOSE WHO HAVE LITTLE.
- (b) The cipher is a keyword columnar substitution cipher with the keyword CHAMPIONS. The plaintext is THE PITTSBURGH STEELERS HAVE WON THE MOST SUPER BOWLS, THE BOSTON CELTICS HAVE WON THE MOST NBA CHAMPIONSHIPS, AND THE NEW YORK YANKEES HAVE WON THE MOST WORLD SERIES.
2. (a) Among other problems, no letter occurs in the plaintext more than once.
- (b) Among other problems, the most commonly occurring letters in the plaintext are F and M, and no digraph occurs in the plaintext more than once.
3. (a) A MWJ AZ UKI SGGY
- (b) I WAS IN THE POOL.
- (c) Superencryption by two substitution ciphers does not in general yield more security than encryption by one substitution cipher. The overall cipher that results from superencryption by two substitution ciphers is itself a substitution cipher.

2.4 A Maplet for Cryptanalysis of Substitution Ciphers

1. (a) TRUE HEROISM IS REMARKABLY SOBER, VERY UNDRAMATIC. IT IS NOT THE URGE TO SURPASS ALL OTHERS AT WHATEVER COST, BUT THE URGE TO SERVE OTHERS AT WHATEVER COST.
- (b) THE PRICE OF SUCCESS IS HARD WORK, DEDICATION TO THE JOB AT HAND, AND THE DETERMINATION THAT WHETHER WE WIN OR LOSE, WE HAVE APPLIED THE BEST OF OURSELVES TO THE TASK AT HAND.
- (c) HOW IMPORTANT ARE THE VISUAL ARTS TO SOCIETY? I FEEL STRONGLY THAT THE VISUAL ARTS ARE OF VAST AND INCALCULABLE IMPORTANCE. OF COURSE I COULD BE PREJUDICED. I AM A VISUAL ART.
2. (a) The cipher is a keyword columnar substitution cipher with the keyword TREASURE. The plaintext is IF YOU CAN BREAK THE BEALE CIPHERS, YOU MAY BECOME A VERY RICH PERSON. HOWEVER, MANY PEOPLE THINK THE BEALE TREASURE IS A HOAX. WE MAY NEVER KNOW FOR SURE.
- (b) The cipher is a simple keyword substitution cipher with the keywords ROCK SONG. The plaintext is JUST SLIP OUT THE BACK, JACK, MAKE A NEW PLAN, STAN, YOU DON'T NEED TO BE COY, ROY, JUST GET YOURSELF FREE. HOP ON THE BUS, GUS, YOU DON'T NEED TO DISCUSS MUCH, JUST DROP OFF THE KEY, LEE, AND GET YOURSELF FREE.
3. TO ME, THERE ARE THREE THINGS WE ALL SHOULD DO EVERY DAY. WE SHOULD DO THIS EVERY DAY OF OUR LIVES. NUMBER ONE IS LAUGH. YOU SHOULD LAUGH EVERY DAY. NUMBER TWO IS THINK. YOU SHOULD SPEND SOME TIME IN THOUGHT. AND NUMBER THREE IS, YOU SHOULD HAVE YOUR EMOTIONS MOVED TO TEARS. COULD BE HAPPINESS OR JOY, BUT THINK ABOUT IT, IF YOU LAUGH, YOU THINK, AND YOU CRY, THAT'S A FULL DAY. THAT'S A HECK OF A DAY. YOU DO THAT SEVEN DAYS A WEEK, YOU'RE GOING TO HAVE SOMETHING SPECIAL.

4. A GOOD GLASS IN THE BISHOP'S HOSTEL IN THE DEVIL'S SEAT, FORTY-ONE DEGREES AND THIRTEEN MINUTES NORTHEAST AND BY NORTH MAIN BRANCH SEVENTH LIMB EAST SIDE SHOOT FROM THE LEFT EYE OF THE DEATH'S-HEAD A BEE-LINE FROM THE TREE THROUGH THE SHOT FIFTY FEET OUT.

2.5 Playfair Ciphers

1. (a) ZTKSKBALBIKBKZKZ
(b) SKBKDQDKQVMIKBKZKZ
(c) SOUTHERN CAL BASEBALL
2. (a) FCZOGOMQZSFELABFISIU
(b) SBSFIHVCSHHEIVABPOSFHWEOHSZ
(c) THE OUTLAW JOSEY WALES IS BETTER YET.
4. LABOULAYE LADY WILL LEAD TO CIBOLA TEMPLES OF GOLD.

2.6 A Maplet for Playfair Ciphers

1. (a) IAGYMRKQSOWDTNSLWMMNHESRHEIANAMRSLQDBOSIMNDFUSCRRV
(b) QMDHNNHAGOENTUOQOGQGMPOYFQFONQSGQINFNFLDSCXCVCNFW
(c) THEY HAVE ALSO WON TEN ACC TITLES AND HAD THIRTEEN ALL-AMERICANS.
2. (a) AQHPNTNQUNPQIFAYFPBBLEZNKMZKGKTGPUGQCCXVRUROEQMKUNUDRAEGIMIINCOQOYAEG
XYQYHGNCNKGRVTIQONDEGXY
(b) QMKPIGFBQMKIVGIGNYQOIMSIGNPYOQZYVGCTNZIMONUBQMEBXCNOEAYCFPBZKGONKGTN
ZINUNFGVLNNKBFUNRVINEGONAQHPNTNQUNEUNKDOMIPQFBUGDOCNGENUNDONKGQYEGDRAE
GI
(c) THERE FOLLOWED A FRANTIC 'DEAR CHARLIE: WRITE NO MORE. OUR CIPHER IS
DISCOVERED!' - AND THEN SILENCE.
4. PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X
CREW OF TWELVE X REQUEST ANY INFORMATION X