Coded Messages ~ 1

Messages which are intended to be kept secret can be sent in code. This requires the sender and recipient to know the same code. Usually this is contained in a book. The one to be used here is **The *Small* Code Book**

Suppose this message has been received and we wish to recover the real message:-

LWBZZ HMZAH XCFZH KAFKG

The *Small* Code Book uses 2-letter groupings so we re-write the message in that way:-

LW BZ ZH MZ AH XC FZ HK AF KG

This is known as the coded text and we wish to change it into plain text.

We now look up the meanings of each of those 2-letter groups (Code to Plain)

LW is can
BZ is you
ZH is bring
MZ is diamonds and so on

The real message is recovered as:-

can you bring diamonds to me by Wednesday 22 October

Notice that real message had 43 letters but was sent by a message of only 20 letters. This is an important use of a code book if the cost of sending a message is worked per letter. In fact, in the early days of message sending, massive code books were produced commercially for that very reason. They were rather like inter-language dictionaries. The first section gave the change from plain text to code, and the second section gave the change from code to plain text. Of course the size of the letter groups was much more than two which only allows 26^2 (676) groups to be used. For serious work the size of the group would be 4 or 5, which allows for the creation of 26^4 (nearly half a million) or 26^5 (nearly 12 million) code groups or words.

Of course there was no secrecy about those codes, anyone could buy the books. But secrecy was not the objective, saving money was. If secrecy was desired, and it was, by both commercial enterprises and national bodies, then the code books had to be produced (and distributed) under conditions of strict security.

Code books are still used but only for some very special purposes. The ready availability of computers linked to modern communication systems allows much more sophisticated methods to be used. They are less labour-intensive too.

Sometimes, no matter how big the code book is, words will be needed which are not in the book and it is necessary to spell them in full. Consider this message:-

UPBNH ZYECT PEPKQ DILYD DBMTA
HGAGH UFTVL AOZOK JCHNI PPEEH

Taking 2 letters at a time and looking them up in the code book recovers:-

gold will be on ship C E R E S *(space)* going
to R O M E *(space)* at 17.00 Monday C P

The C P on the end could be a signature, or merely nulls to make up the 5-group.

© Frank Tapson 2003 [trolC3:1]

Coded Messages ~ 2

Exercise 8

Use The *Small* Code Book to decode these messages

1. SSDZS XHRGN WNEKJ JXAIP
2. NZNGC MDGQW EQQJZ BCOPA
3. NFQWA JLCPZ TMDNF NRXTD
4. QPAHO CZCRN ORMZK MNMQC YMQVT XEKJL XLFQF ZWNOL
5. PZYLN XWXEC ZJTDO RZMNC YHBZL WWVZH NFSAN EWYCY
6. KSYLI NWAES YNBZX DCSSC XCHJT
   TRKUA QZORN HHKVY BCITU MCFBZ
7. BZCON NVHWV ZMUKF NKSYL AXAPK
   KPPEN KFNHH RTWOG IEAKF
8. DZDGJ LRCUB FYBNN ULXEH GAESP ESFRH
9. YNXCW WEBPM YDRHJ CUFLX QDMWH XENJU HRVQO RHZOO
10. WDJLR JAYBS YEGNK RORQP ECYBH
    RUFES YRJXT VGAXG WTSCR WLXSP

© Frank Tapson 2003 [trolC3:2]

Coded Messages ~ 3

Extracts from The *Small* Code Book

CODE → Plain

AF 22
AH to
AJ men
AK
AL position
AO in
AP •
AX guarded
AY thousand

BC let
BN will
BO 6
BQ help
BS pound
BX was
BZ you

CF follow
CJ A
CL you
CM know
CO must
CS look
CT ship
CY •

DD
DG all
DM torch
DN prison
DT my
DX but
DZ for

EB church
EC to
EE patrol
EH P
EK East
EN at
EQ secret
ER city
ES I
EW 10

FE half
FN •
FQ tree
FV right
FY word
FZ by

GA R
GB arrest
GC dawn
GE Thursday
GH O
GJ 20
GN your
GT found
GX ferry
GY they

HD centre
HJ inside
HK Wednesday
HO telephone
HR on
HU road
HX S
HZ be

IE June
IL E
IN urgent
IP Monday
IT no

JC •
JF why
JJ border
JK van
JL of
JU sunset
JX B

KE signal
KF 23
KG October
KJ key
KK do
KM necklace
KQ year
KR head
KS it
KW wireless
KZ nuclear

LA
LC are
LO since
LS curfew
LW can
LX A
LZ bridge

MF people
MJ D
MT going
MW K
MZ diamonds

NC first
NE with
NF all
NG police
NH 00
NL radio
NM is
NN cross
NP gram
NS of
NU be
NZ the

OC old
OE gates
OG 9
OL wall
OO careful
OP tanks
OR •
OZ at

PA fly
PE C
PF wanted
PK E
PM of
PP it
PZ now

QC 15
QD R
QG danger
QJ so
QM school
QP go
QV North
QW our
QZ 18

RC March
RH T
RJ one
RK stations
RN gardens
RW J
RX run

SA gang
SC for
SP N
SS watch
SX attack

TD away
TM in
TT railway
TU private
TV E
TW Sunday
TX 8

UA about
UB pass
UF M
UH kilo
UK care
UM one
UP gold
UQ who
UV bus

VB flag
VH frontier
VQ Friday
VY •

WA that
WD reward
WN South
WT ask
WV •
WW outside
WX time
WY guns

XA next
XC me
XD •
XG street
XL orange
XQ guard
XV silver

YB house
YD S
YE on
YH train
YL is
YM metres
YN see
YR L
YU shell

ZB we
ZC castle
ZH bring
ZJ get
ZM take
ZQ policeman
ZW million

© Frank Tapson 2003 [trolC3:3]