

Extended Handycipher

Extended Handycipher operates with the same plaintext and ciphertext alphabets, and encrypts a message M using a key K by first generating a random session key K' and encrypting M with Handycipher using K' to produce an intermediate ciphertext C' . K' is then encrypted with Handycipher using K and embedded in C' at a location based on K and the length of M , producing the final ciphertext C .

Extending Handycipher in this way confers several advantages in security at little computational cost. Because each plaintext message is encrypted with a different randomly generated session key, the primary secret key is less exposed to any attack that depends on having a lot of ciphertext to work with, and the security of the cipher is less compromised by encrypting multiple messages with the same key.

Extended Handycipher encryption algorithm: $C \Leftarrow E^*(K, M)$

1. Generate a random 41-character key K' with associated table $T_{K'}$ and coding substitution $\xi_{P'}$.
2. Encrypt M with Handycipher and K' , yielding C' .
3. Transcribe K' into plaintext characters by spelling the ten digits and the word “space” and enclose each spelled word in a pair of spaces.
4. Encrypt the transcribed K' with Handycipher and K , yielding K'' . Adjust K'' if necessary ensuring that for the last character m of the transcribed K' to be encrypted, no null characters are interspersed with $\sigma(m)$ and that K'' terminate with exactly one null character.¹
5. Adjust C' if necessary, by inserting more nulls, ensuring that $|C'| + |K''| \geq 500$ and also that $N \geq 30 - R$ where $|C'| = 31 \cdot N + R$, $0 \leq R < 31$.
6. Calculate $j = \lfloor (|C'| + |K''| - 500) / 31 \rfloor \cdot \{[\xi_{P(A)} + \xi_{P(B)} + \xi_{P(C)}] \bmod 31\} + [\xi_{P(D)} + \xi_{P(E)} + \xi_{P(F)}] \bmod 31$.²
7. Insert K'' into C' immediately following position j as calculated in step 6, yielding C .

Extended Handycipher decryption algorithm: $M \Leftarrow D^*(K, C)$

1. Calculate $j = \lfloor (|C| - 500) / 31 \rfloor \cdot \{[\xi_{P(A)} + \xi_{P(B)} + \xi_{P(C)}] \bmod 31\} + [\xi_{P(D)} + \xi_{P(E)} + \xi_{P(F)}] \bmod 31$ and begin decrypting the substring of C immediately following position j with Handycipher and K .
2. Transcribe the spelled digits and the word “space” back into their ciphertext character equivalents.
3. Continue until 41 such characters have been decrypted, yielding the session key, K' .
4. Remove the decrypted substring from C , leaving C' .
5. Decrypt C' with Handycipher and K' , yielding M .

¹ This is necessary so that in Step 3 of the decryption algorithm the end of K'' can be recognized.

² Here $\lfloor x \rfloor$ denotes the integer part of x and $|C|$ denotes the length of C . The formula is designed merely to make the value of j depend on K (and its subkey P) and $|C|$. The adjustments in Step 5 ensure that $j \leq |C|$.

Example encryption with Extended Handycipher

Continuing with the previous Handycipher example, to encrypt the Williams quote with Extended Handycipher, at first a random 41-character session key K' is generated, say:

Z D B 9 H A ? G V 8 1 J M T O U K - Y 5 0 Q 4 L ^ W F E R 6 I N . C , 7 2 X S 3 P

with subkey P'

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

and associated table $T_{K'}$

Z	D	B	9	H	A	?	G
V	8	1	J	M	T	0	U
K	-	Y	5	0	Q	4	L
W	F	E	R	6	I	N	.
C	,	7	2	X	S	3	P

and coding substitution $\xi_{P'}$

m: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z , . - ? ^
 $\xi_{P'}(m)$: 5 3 27 2 22 21 7 4 24 9 14 18 10 25 12 31 17 23 30 11 13 8 20 29 16 1 28 26 15 6 19

The quote³ is then encrypted with Handycipher using this $\xi_{P'}$ and $T_{K'}$, yielding, for example, this 1041-character ciphertext as C'

,CQ8B I46GJ MUVAY 25WRE .DOCQ 1K-S5 4HV-G EX,P. C-508 LTM1K ?B8.9 UGP1X 4MJ85 HYFP1 DC9SP XTI-W N15ZR TFSWE XA-WS 1,5AI .QD51 0R3D, ATZM4 Y8,AZ 57DUR OBQWJ DPZRJ G6H0S FN?7N MIOD7 3RF,4 SMVJW FRTKE ,A17B 5INM. ?LE7F 9EIB1 ZMQR. ?8HIF 3YTSG 6?WPF 1BX40 M67UR DEPW. IHX6S 38LR- UN9W3 M.,N5 Z1E7N BPN,S .GWRU WY?CQ JK8B6 Y01U7 EKP50 0Z9IA DPK,E 10ADC 9MK.H 6MP20 HV,3C ?8VM6 82NY4 VHKL5 0156P J2U9E GZQN0 57XCQ EFU6Z WNCR6 AUV1J 89?7U MCPY6 WTF0? P.TDO NRVT. 7-YK0 41Y3P .0S6U PFR?W 5GR98 62KE. WFRHI CJ-PQ 1ZNKC T4E7B M98UT GLXY9 M7K1B PG7WX ?L71B J95AU ?HCSF 4QS1J -.U0? KD4HU BOM9T KIFQ5 SMA,C L2.YQ STZX5 I0KPG E?LYT ,7XNV IJ82S ACLNX UK98B 2M4I2 6B?.Q RAS8Z -KLEV SFHYL 92JZ? T80.? AY-5X W.938 Z0?R4 K.JS2 5HOX6 3G7X. CNMTO Z7,PX I?NC0 6H7DV F6ARK SXYGT 9RJ6X A4QHV HKSML 7I8UT PSKB2 3WFN6 YE0G7 1,?.I ZTG4E UXDB- GF.DM ZUECX ,R420 RUNDQ X.2,1 .9XTJ B?8MU VA,3. JSWUI 4YSV. 8TI?W RL6IB D9V.Z CMFN4 G7-.? B9AQZ 24HUT V95RJ ZKPSV WCB1Z Y8XV3 ?U.8F HJ7BS EU?IW S3.Q0 ZP0,5 48,UD AP9GT DQWEK 0-CHJ K-MLT 6P0XC 4LUZW -4DWO RP67L ,CMKJ 16VZC 04,LQ 103,M E5WHQ FUYN? .VQKN 3LZIO ?C9?P NFG?O MKN1V B624T K,ITR 0.4J9 ,ZOIM 6QHXB 0WJRA V0AQ7 S8B2W 1IX03 BHQ?D XNLHM .KOU? U05N6 BGUON KRXGY I4T8H V-E80 P?KS2 FA9KS GQXZ8 CUI07 UAE7Q 6H.8M TD3VP B00F3 8E2VG
parsed as:

³ A dash is included in the plaintext word “ad-versary” because this choice of key does not allow the bigram DV to be encrypted (see footnote 3 of the Handycipher description).

I t ^ h a u n t s ^ m e ,
 ,C Q8BI46 GJMUAY 25 WRE .DOCQ1 K-S5 4HV-GE X,P.C -5 08LTM1 K?B8
 ^ t h e ^ p a s s a g e
 .9UGP1X 4MJ8 5 HYF P1DC 9SPXTI-WN1 5Z RTFSWE XA-WS1 ,5 AI.QD51 0R3D
 ^ o f ^ t i m e . ^ I ^ t h i
 ,ATZM 4Y8 ,AZ5 7DUR OBQWJ DPZ RJ G6H0 SFN?7NM IOD73R F, 4SMVJ WFR TK E,
 n k ^ t i m e ^ i s ^ a ^
 A17B 5INM.?LE 7F9 EIB1 ZM QR.?8 HIF3Y TSG6?WPF 1B X40M6 7URD EPW .IHX6
 m e r c i l e s s ^ t h
 S38LR -UN9W 3M.,N5Z 1E7NB PN,S.GW RUW Y?CQJ K8B6 Y01U7E KP50 OZ9IAD PK
 i n g . ^ I ^ t h i n k ^ l i f
 ,E 10ADC 9MK .H6M P20HV ,3C ?8VM 682 NY 4VH KL50 156 PJ2U9 EGZ QN05 7XC
 e ^ i s ^ a ^ p r o c
 QEFU6 ZWNC R6 AUV1J8 9?7UM CPY 6WTF 0?P.TDONRTV.7 -YK0 41Y 3P.OS6UPFR?W
 e s s ^ o f ^ b u r n i n g
 5GR9 862K E.WFR HICJ -PQ1 ZNKC T4E7B M9 8UTGLXY 9M7K 1BPG7 WX ?L71B J95
 ^ o n e s e l f ^ o u
 AU?HCSF 4QS1J -.U0?K D4HUB 0M9TKIF Q5SMA, CL2 .YQSTZX 5I0K PGE?LY T,7X
 t ^ a n d ^ t i m e ^ i s
 NVIJ8 2SACLNX UK9 8B2 M 4I26B ?.QRAS8Z -K LEV SFHY L92J Z?T8 0.?AY-5
 ^ t h e ^ f i r e ^ t h a
 XW.9 38Z0?R 4K .JS25 HOX6 3G7X.C NMT0Z 7,PXI?NC 06H 7DV F6AR K SXY
 t ^ b u r n s ^ y o u .
 GT9RJ 6XA4QH VH KSML7 I8UTPSKB2 3WFN6 YE0G71 ,?.IZTG4E UX DB -GF.D MZUE
 ^ B u t ^ I ^ t h i n k ^
 CX, R42 0RUND QX.2, 1.9X TJB ?8MUV A,3.JSW UI4Y SV.8 TI?WRL6 IBD9 V.ZC
 t h e ^ s p i r i t ^ o
 MFN4G7 - .?B9AQZ 24HUTV 95RJ ZKPSVWC B1 ZY8X V3?U.8 FHJ 7BSE U?IWS3.Q0
 f ^ m a n ^ i s ^ a ^ g o o d
 ZP0,5 48,UD AP9GTD QWE K0- CHJ K- MLT6P0X C4LUZW -4D WORP6 7L,C MK J1 6
 ^ a d - v e r s ^ a r y
 VZC 04, LQ1 03,ME5 W HQFUY N?.VQKN3LZI0?C 9?PNFG?OMK N1V B624TK ,
 . ^ - ^ T e n n
 ITRO.4J9 ,ZOIM 6QHX B0WJ RAV0AQ7 S8B2 W1IX 03BHQ?D XNLHM .KOU?U05
 e s s e e ^ w i l l i a
 N6BGUONK RXGYI4T8 HV-E 80P?KS2 FA9K SGQXZ8 CUI07 UAE7 Q6H .8M TD3V PB00
 m s
 F38 E2VG-

K' is transcribed into plaintext characters as

ZDB nine HA?GV eight one JMTOUK-Y five zero Q four L space WFER six IN.C, seven two XS three P

and then encrypted with Handycipher and K'' , for example,

?X0ZW QYC5T LS8JZ C2316 0HG0. MN5UI XKQPC JZVS5 ?9CRL 70T5, A24LF MTBV2 KXA23
 QU,HI -SZ.J CN7OH FYNSP T?MWJ P459? T1.YC UP?9F ,4NE6 C71GN 8W9MG 6BS01 4P37,
 U2-5Q 4.UG1 OZ.WG HLC9V G5W81 4T?W9 N5X1- NVS?G .5-VX BA.NH 5X0-6 48HBD PMEYP
 H34RP WE1BM EU50A YTSY- 70BF5 TZ10S T-YJ. NH520 HL8ZG N-QJY I48HG UW,SF MKJVS
 PTS0V BX49M QZQ1X A8TFK HNBMO G2VBC UVIFZ .Y5ZA XF9U6 B?.QE 7W9I5 LZ3T. 02LX4
 E

The position at which the encrypted session key will be inserted is calculated as

$$\begin{aligned} j &= \lfloor (|C'| + |K''| - 500) / 31 \rfloor \cdot \{[\xi_p(A) + \xi_p(B) + \xi_p(C)] \bmod 31\} + [\xi_p(D) + \xi_p(E) + \xi_p(F)] \bmod 31 \\ &= \lfloor (1041 + 326 - 500) / 31 \rfloor \cdot \{[13 + 31 + 14] \bmod 31\} + [7 + 16 + 5] \bmod 31 \\ &= 27 \cdot 27 + 28 \\ &= 757 \end{aligned}$$

K'' is inserted following the 757th character of C' , yielding C

,CQ8B I46GJ MUVAY 25WRE .DOCQ 1K-S5 4HV-G EX,P. C-508 LTM1K ?B8.9 UGP1X
 4MJ85 HYFP1 DC9SP XTI-W N15ZR TFSWE XA-WS 1,5AI .QD51 0R3D, ATZM4 Y8,AZ
 57DUR OBQWJ DPZRJ G6H0S FN?7N M10D7 3RF,4 SMVJW FRTKE ,A17B 5INM. ?LE7F
 9EIB1 ZMQR. ?8HIF 3YTSQ 6?WPF 1BX40 M67UR DEPW. IHX6S 38LR- UN9W3 M.,N5
 Z1E7N BPN,S .GWRU WY?CQ JK8B6 Y01U7 EKP50 0Z9IA DPK,E 10ADC 9MK.H 6MP20
 HV,3C ?8VM6 82NY4 VHKL5 0156P J2U9E GZQN0 57XCQ EFU6Z WNCR6 AUV1J 89?7U
 MCPY6 WTF0? P.TDO NRVT. 7-YK0 41Y3P .0S6U PFR?W 5GR98 62KE. WFRHI CJ-PQ
 1ZNKC T4E7B M98UT GLXY9 M7K1B PG7WX ?L71B J95AU ?HCSF 4QS1J -.U0? KD4HU
 BOM9T KIFQ5 SMA,C L2.YQ STZX5 I0KPG E?LYT ,7XNV IJ82S ACLNX UK98B 2M4I2
 6B?.Q RAS8Z -KLEV SFHYL 92JZ? T80.? AY-5X W.938 Z0?R4 K.JS2 5H0X6 3G7X.
 CNMTO Z7,PX I?NC0 6H7DV F6ARK SXYGT 9RJ6X A4QHV HKSML 7I8UT PSKB2 3WFN6
 YEOG7 1,?.I ZTG4E UXDB- GF.DM ZUECX ,R420 RUNDQ X.2,1 .9XTJ B?8MU VA,3.
 JSWUI 4YSV. 8TI?W RL6IB D9V.Z CMFN4 G7-.? B9?X0 ZWQYC 5TLS8 JZC23 160HG
0.MN5 UIXKQ PCJZV S5?9C RL70T 5,A24 LFMTB V2KXA 23QU, HI-SZ .JCN7 OHFYN
SPT?M WJP45 9?T1. YCUP? 9F,4N E6C71 GN8W9 MG6BS 014P3 7,U2- 5Q4.U G10Z.
WGHLC 9VG5W 814T? W9N5X 1-NVS ?G.5- VXBA. NH5X0 -648H BDPMF YPH34 RPWE1
BMEU5 0AYTS Y-70B F5TZ1 0ST-Y J.NH5 20HL8 ZGN-Q JYI48 HGUW, SFMKJ VSPTS
0VBX4 9MQZQ 1XA8T FKHN B MOG2V BCUVI FZ.Y5 ZAXF9 U6B?. QE7W9 I5LZ3 T.02L
X4EAQ Z24HU TV95R JZKPS VWCB1 ZY8XV 3?U.8 FHJ7B SEU?I WS3.Q 0ZP0, 548,U
DAP9G TDQWE K0-CH JK-ML T6P0X C4LUZ W-4DW ORP67 L,CMK J16VZ C04,L Q103,
ME5WH QFUYN ?.VQK N3LZI 0?C9? PNFG? OMKN1 VB624 TK,IT R0.4J 9,ZOI M6QHX
B0WJR AV0AQ 7S8B2 W1IX0 3BHQ? DXNLH M.KOU ?U05N 6BGUO NKRXG YI4T8 HV-E8
OP?KS 2FA9K SGQXZ 8CUIO 7UAE7 Q6H.8 MTD3V PB00F 38E2V G-