**V15**

WQV WVSVJITUQ ztov hifuwnjituqf rqtw xw xp wnotf. Ptzdvs C. A. Znipvpvgw "Rqtw qtwq Jno

rindjqw!" xg 1844. Wqv gvyw fvti qxp strfvi tgouinznwxngts tjvgw, Citghxp N. E. Pzxwq, udasxpqvo

t hnzzvihxts hnovvgwxwsvo Wqv Pvhivw Hniivpungoxgj Knhtadstif; Totuwvo cni Dpv wn

Znipv'pVsvhwin-Ztjgvwxh Wvsvjituq, xg rqnpv uivcthv qv ovhstivo wqtw "pvhivhf

xghniivpungovghv, xp cti wqv znpw xzuniwtgw hngpxovitwxng." Wqxp rtpuinkxovo af t pduvi-

vghxuqvizvgw.Tp wqv znpw vyhxwxgj xgkvgwxng nc wqv cxipw qtsc nc wqv hvgwdif,

wqvwvsvjituq pwxiivo tp zdhq xgwvivpw xg xwp otf tp Pudwgxl oxo xg xwp. Wqvjivtw tgo rxovsf

cvsw gvvo cni pvhivhf trtlvgvo wqv stwvgw xgwvivpw xghxuqvip wqtw pn ztgf uvnusv pvvz wn

qtkv, tgo lxgosvo t gvr xgwvivpw xgztgf nwqvip. Onmvgp nc uvipngp twwvzuwvo wn oivtz du wqvxi

nrgdgaivtltasv hxuqvip. Wqvxi hngwixadwxngp vgixhqvo xw rxwq onmvgp nc gvrhxuqvi

pfpwvzp.Tp adpxgvppzvg tgo wqv udasxh dpvo wqv wvsvjituq zniv tgo zniv,wqvf cndgo wqtw

wqvxi cvtip tandw sthl nc uixkthf rviv vytjjvitwvo. Wqvhsvilp ovtsw xzuvipngtssf rxwq wqv

zvpptjvp. Wqv wvsvjituq hnzutgxvpivpuvhwvo wqvxi hngcxovgwxtsxwf. Tgo hnzzvihxts hnovp sxlv

Pzxwq'p, rqxhqivusthvo rniop tgo uqitpvp af pxgjsv hnovrniop ni hnov-gdzavip wn hdw wvsvjituq

wnssp, tccniovo pdccxhxvgw pvhdixwf cni znpwadpxgvpp witgpthwxngp af pxzusf uivhsdoxgj tg

tw-pxjqw hnzuivqvgpxng ncwqv zvtgxgj. Wqv ainlvip tgo witovip pnng ivtsxmvo wqtw wqv

ztxgtoktgwtjv nc wqvpv hnovp rtp wqvxi vhngnzf.Jnkvigzvgw zxgxpwixvp dpvo wqv wvsvjituq,

wnn. Tw cxipw wqvf zdpwqtkv vghnovo rxwq wqvxi gnzvghstwnip. Adw tswqndjq pvhivhf

rtputitzndgw cni wqvz, wqvf sxlvo wqv wvsvjituqxh vhngnzf nc t stijv hnov—vpuvhxtssf tp wqvf

wvsvjituqvo zniv tgo zniv. Pn rqvg wqv wxzv tiixkvown hnzuxsv t gvr gnzvghstwni, wqvf tatgongvo

wqtw cniz, hnuxvo wqvhnzzvihxts cniz, tgo uinodhvo t cdss-csvojvo hnov. Wqv gnzvghstwnipqto

qto wqvxi 1,- ni 2,000 hnov-gdzavip xg zxyvo niovi, adw wqv rtitgo cnivxjg zxgxpwixvp atslvo tw

wqv vyuvgpv nc oitrxgj du t 50,000-vgwif hnov xg wrn utiwp, tgo wqvf qto gn uincvppxngts

hifuwtgtsfpwp wnrtig wqvz nc wqv otgjvi nc wqv ngv-utiw cniztw. Wqvf ivsxvo cni pvhdixwfdung

pztss voxwxngp, axj ptcvp, vywvgpxkv svyxhng (stijv hnovp tiv qtioviwn aivtl wqtg pztss ngvp,

nwqvi wqxgjp avxgj vbdts), tgopduvivghxuqvizvgw, ivwtxgxgj hnovgdzavip wn cthxsxwtwv wqxp

xgpwvto ncprxwhqxgj wn hnovrniop. Wqxp vknsdwxng rtp vppvgwxtssf hnzusvwv af wqv1860p.

Wqv stijv, ngv-utiw hnov qto ivusthvo wqv pztss, wrn-utiwgnzvghstwni xg qxjq-svkvs zxsxwtif tgo

oxusnztwxh hifuwnjituqf.Zvtgrqxsv, wqv wvsvjituq, tdwqni nc wqxp ovkvsnuzvgw, rtp

hivtwxgjpnzvwqxgj gvr xg rti—pxjgts hnzzdgxhtwxngp, ni knsdzxgndp hnzztgotgo ivhnggtxpptghv

zvpptjvp. Nc hndipv pdhq zvpptjvp qto vyxpwvoavcniv, rxwq wnihqvp, uxjvngp, tgo hndixvip, adw

xg pn itivcxvo t cniz wqtwwqvf rviv gnw vkvg htssvo "pxjgts hnzzdgxhtwxngp." Wqv

wvsvjituqvgtasvo hnzztgovip, cni wqv cxipw wxzv xg qxpwnif, wn vyviw xgpwtgwtgvndptgo

hngwxgdndp hngwins nkvi jivtw ztppvp nc zvg puivto nkvi stijvtivtp.Wqvpv wthwxhts zvpptjvp

ivbdxivo uinwvhwxng: wvsvjituq rxivp hndso avwtuuvo. Gvxwqvi wqv nso gnzvghstwni gni wqv

gvr hnov rndso on. Wqvfrviv wnn vtpf wn htuwdiv xg hnzatw, wnn qtio wn ivxppdv bdxhlsf

tgocivbdvgwsf wn wqv gdzvindp tgo rxovpuivto wvsvjituq unpwp. Pxjgtsnccxhvip wdigvo trtf cinz

wqvz. Wqvf snnlvo xgpwvto wn wqtw gvjsvhwvohqxso nc hifuwnjituqf, wqv hxuqvi. Hxuqvip hndso

av uixgwvo hqvtusf ng tpxgjsv pqvvw nc utuvi tgo oxpwixadwvo rxwq vtpv. Pvhivhf rtp atpvo

dungktixtasv lvfp, pn htuwdiv nc wqv jvgvits pfpwvz tgo vkvg nc ngv nc wqvlvfp rndso gnw

hnzuinzxpv tss tg tizf'p pvhivw zvpptjvp. Pnsdwxngprndso av uivkvgwvo af ituxo lvf hqtgjvp.

Hxuqvip rviv xovts cni atwwsv-mngv zvpptjvp, tgo wqv cxipw nc wqv znovig rtip, wqv Tzvixhtg

Hxkxs Rti,dpvo wqvz cni edpw wqtw. Wqdp rtp anig t gvr jvgiv xg hifuwnjituqf: wqvcxvso hxuqvi.

**Decrypted**

the telegraph made cryptography what it is today. samuel f. b. morsesent "what hath god

wrought!" in 1844. the next year his lawyer andpromotional agent, francis o. j. smith, published

a commercial codeentitled the secret corresponding vocabulary; adapted for use to

morse'selectro-magnetic telegraph, in whose preface he declared that "secrecy

incorrespondence, is far the most important consideration." this wasprovided by a super-

encipherment.as the most exciting invention of the first half of the century,

thetelegraph stirred as much interest in its day as sputnik did in its. thegreat and widely

felt need for secrecy awakened the latent interest inciphers that so many people seem to

have, and kindled a new interest inmany others. dozens of persons attempted to dream up their

ownunbreakable ciphers. their contributions enriched it with dozens of newcipher

systems.as businessmen and the public used the telegraph more and more,they found that

their fears about lack of privacy were exaggerated. theclerks dealt impersonally with the

messages. the telegraph companiesrespected their confidentiality. and commercial codes like

smith's, whichreplaced words and phrases by single codewords or code-numbers to cut telegraph

tolls, afforded sufficient security for mostbusiness transactions by simply precluding an

at-sight comprehension ofthe meaning. the brokers and traders soon realized that the

mainadvantage of these codes was their economy.government ministries used the telegraph,

too. at first they musthave encoded with their nomenclators. but although secrecy

wasparamount for them, they liked the telegraphic economy of a large code—especially as they

telegraphed more and more. so when the time arrivedto compile a new nomenclator, they abandoned

that form, copied thecommercial form, and produced a full-fledged code. the nomenclatorshad

had their 1,- or 2,000 code-numbers in mixed order, but the warand foreign ministries balked at

the expense of drawing up a 50,000-entry code in two parts, and they had no professional

cryptanalysts towarn them of the danger of the one-part format. they relied for securityupon

small editions, big safes, extensive lexicon (large codes are harderto break than small ones,

other things being equal), andsuperencipherment, retaining codenumbers to facilitate this

instead ofswitching to codewords. this evolution was essentially complete by the1860s.

the large, one-part code had replaced the small, two-partnomenclator in high-level military and

diplomatic cryptography.meanwhile, the telegraph, author of this development, was

creatingsomething new in war—signal communications, or voluminous commandand reconnaissance

messages. of course such messages had existedbefore, with torches, pigeons, and couriers, but

in so rarefied a form thatthey were not even called "signal communications." the

telegraphenabled commanders, for the first time in history, to exert instantaneousand

continuous control over great masses of men spread over largeareas.these tactical messages

required protection: telegraph wires could betapped. neither the old nomenclator nor the

new code would do. theywere too easy to capture in combat, too hard to reissue quickly

andfrequently to the numerous and widespread telegraph posts. signalofficers turned away from

them. they looked instead to that neglectedchild of cryptography, the cipher. ciphers could

be printed cheaply on asingle sheet of paper and distributed with ease. secrecy was based

uponvariable keys, so capture of the general system and even of one of thekeys would not

compromise all an army's secret messages. solutionswould be prevented by rapid key changes.

ciphers were ideal for battle-zone messages, and the first of the modern wars, the american

civil war,used them for just that. thus was born a new genre in cryptography: thefield cipher.

