

Forum:[Hack Forums](#)

Thread: [Encryption Challenge:](#)

arcticbear - October 7, 2024, 2:19 pm

Hey everyone,

I've been working on a new encryption algorithm and would love to see if anyone here can crack it. Below are two encrypted versions of a message, each using a different key. I believe it's nearly impossible to break due to the high chance of false positives.

Encrypted Message 1:

8/'Jwfnlq=%K;dVu>mPu)-=;MN* RiLNU8Guhb!ROha#GkY,l<|F+B\u007frur@+\"UG5.rw*LaN)
\\#p({HDFG*_M3(df@a&q'rUn\\5f\$)yS*IBd)_aa^`xf.]n<+];UX}WgygxJF\_+uSUBsp;Pg<|]a7[+<vK>!7`
#hDzC`i>:Q\\#0#hHJ]2*?MGR2Z\u007f?Vv#1<x)pD?f}DSo%1P:*T9Nllvb{hTCUjSdANE
oxUF_+4;U_bkP^+\${l0w/<uFW`j}).Dq\u007fw},.^F\"On{Sm^`nJI/V<C\"<?|!rHJ3zUU5p\$}BLoUMCX4{
nN>FvCTYDFh
)g}iCm4Wk(.c.S7*DjQR<XZa1[PVd\\QN\$U\u007ffit\"Aw.7M7GOH7qHWTq\u007fy{*Ydf{;S\u007f^r(L
921FXn>nPU<~%*V>qP-)d':+Y>*R`6os/vfAF\"OqPe<`jf7WB:x@MgV-d\\QN2e8\"rgk<4,M?D}0@(SP
Ox-y9'#W;/BHZz^~ay!.Fy/B; }UC;:u
ogla-YidIRxZF}Y?8\\P,3!RodaBH!mW1\\\"tRw\$K[u^%\$\$bXh{Lk<4,Mo-\$f#SH%FAek
<KWY'=Oq#\\-3[TFOW,l0bZfq&\u007f-LFF\\\"L)O2
UIUuwB1?us6#UPU\\G/!S6<|Z\$7gKIYY>S%MEhn&S}gNmawD?t#a@A21UL*y5<LO!Md;-&sGkjID>
B})V|XMen^,m?Hw\"9+2gUi0NsCvW,|. %4d`l<+SiC>l0mYD}^

Encrypted Message 2:

BWARvsD|px{;#tW)=cXT5 YiWv8~<4@qvay
fiDVKu.N`M\u007f1T[8QMEfo4d?M+OfT\\the&]N(dwu\$ju_kQ4\"6
q_O/X:EIJP5o?@6eE,Pp*h;vg?Ljn!Kz@n\\N2EUr[P*qs?QdbK@-OLqRdOw[8ZK{c2A]7}\"KXX%p?)
B7.-wuS\$C_GEL\"_ Ng
,3NW1/8v~.r6#sEtPn{ckS{Yb\$9bAl:1'(UpwqYq7X1?0dbKBHO_HML\\a/G{ }\u007f`44;P=<SyF&=P/B
YC^h@kw\u007fv%h0_Sb,u\\kfWj4[z2:DeY@YeE~hnH1K.4]k\$F^As(Vox/~.c|fO<_1`(CHc-
n.r>y.[,>K3c*TjY,J5slu007fh_j6%Y#E&|kBC0_i=XJGr|a_O<!t|RJVR-i[J%Di%iH-tz{d=wXF5a[gHc5S<
(1W@Qn~?d\\\"Aa*/Kf,xazqhP.R%#\"jY,J{cu>t%56+CEcR{S7.tWX*sGZU5QVt@q}kQM6fVEJ(\$~IVH
R#S6)|>5b> Z
YKicLt[EWA2.toDV(a.Le=F-z-Y_v\u007f-p2wNUM56A%<\u007f56+CE?4<0\$V_tQ#Uc-u\$Q_;8lE/qz}
LA_J\$FVhr\\\"!f7.8~BI^2k[U73N~UTddV5\$O\u007fyO|F*On`]Fv<[8>D{%pJ0 }4i
L%+2,BWN<S?rl~@6o%L6/c|<\u007ff{\\4?V%z|y
r_-MiaV3L).\$^kjp[n,G40NNyU4Sq@in1tQC^Ba)l/=svduy{ }ooy,\u007f

I won't be revealing the algorithm itself since I believe it has revolutionary potential, but I'm happy to provide hints if needed. This could include additional examples of the same message encrypted with different keys or a mathematical estimation of the number of combinations required for brute-force attempts.

I'm really curious to know if this kind of algorithm has any practical use or if anyone would be interested in collaborating to explore it further.

Let me know if you can crack it or have any thoughts on its potential applications.

Thanks!

GFMM

sickofit - October 7, 2024, 6:42 pm

(Oct 7, 2024 02:19 PM)arcticbear Wrote: [\[CITE\]](#) I won't be revealing the algorithm itself since I believe it has revolutionary potential

My dude, look into Kerckhoffs's Principle

Delfin - October 8, 2024, 12:17 am

(Oct 7, 2024 02:19 PM)arcticbear Wrote: [\[CITE\]](#) I won't be revealing the algorithm itself since I believe it has revolutionary potential, but I'm happy to provide hints if needed.

This is not something you want to do if you supposedly have a revolutionary algorithm. Like the guy above said, the security of the encryption shouldn't depend on the actual implementation being private - only on the encryption keys used. There's a reason all major encryption algorithms are heavily documented and fully open-sourced - so vulnerabilities can be found, documented and thereafter fixed.