

Forum: [Hack Forums](#)

Thread: [Cracking an encryptions key from weak fixed length outputs](#)

requiem331 - October 9, 2016, 9:11 pm

So lets say that you have a server that generates fixed length tokens. You do not know how the encryption works or what voodoo they do on the server side but you can see as many tokens as you want. How would you go about recovering the key? There is an obvious notable pattern repeated in each token that remains constant. Here are 5 tokens:

383174918c75411045980332d94920984c58425397f96358615f67862586e31f42f54395b59744085a75407675f36683

389105946c20472098900305d68978990c05490367f49399652f00894560e02f41f88361b85746014a05496668f37602

346181954c17479090938340d58966993c07466331f96366653f83881516e75f52f58346b44777023a79430610f04691

384142926c51419089961394d23944936c62443379f00306625f32897544e23f72f70344b75798032a19444679f67618

391106971c03474074949311d31947984c29496366f41301657f88876545e46f62f24366b33740033a86482614f49636

and 5 more:

348111952c67411090953358d46945994c83461330f47322637f35889550e22f74f09326b02744036a64421699f63624

370136986c55492071911351d99964962c77447355f99313683f54801553e71f13f00309b67753023a25437642f60601

303103986c25494009969371d99936971c17455369f89320654f15808553e51f91f08367b46737026a55472675f22646

371159958c08457056970383d71948998c21474377f78372662f28871562e21f09f99313b11738082a21434617f85623

362102970c38476088994326d15976952c93403321f51360637f78814575e66f55f47325b26780031a98451627f12609

It is a digit we know will be there, followed by 8 unknown/random digits, followed by a character we know, and 8 more random digits etc..

How would you go about cracking the key?

chick3nman - October 10, 2016, 12:11 am

This doesn't really look to be keyed right off the bat, and seems more like some kind of information

strip than it does like a unique key. It looks somewhat like numeric data from a magnetic strip track written without formatting. What sort of token is it? And does the oracle confirm validity or simply generate a valid one? Does it hold information or simply authenticate something through unique ID?

requiem331 - *October 10, 2016, 10:15 am*

Well, it is part of a little challenge. All we get is an html page with 2 buttons and a form. The form has a box labeled 'key' and a submit button labeled 'Complete Challenge'. Then under the form is a button called 'Generate Tokens'. Maybe I am missing something and I can find out more about the scheme used.