

Forum: [Hack Forums](#)

Thread: [FBI Dot cryptography problem](#)

Faceless Man - August 8, 2019, 2:55 am

So I was looking for unique cryptography problems a while back, stumbled upon this problem, finally I've been able to figure out the rules for it.

The answer was already available at the bottom of the screen, it was figuring out the rules that was the challenge.

I finally found the answers though, I was never able to find published answers for this.

Here is the link: <https://www.fbi.gov/news/stories/can-you-crack-a-code>

Either way, if someone can find the answers then oh well, least I know myself that I cracked it :D

ApL1e - August 8, 2019, 3:16 am

yeah the fbi is cool they will catch you so don't fuck around kids!

Phizo - August 8, 2019, 9:22 am

I'm pretty disappointed that the FBI would post such a trivial puzzle. This can be solved using introductory-level cryptanalysis; more precisely, you can solve this at not much more than a glance if you've ever done any basic cryptanalysis (the type of cryptography you break at the back of a newspaper — I'm not joking), as this simple puzzle is akin to the first (and extremely basic) cipher you would've encountered anywhere relevant to cryptography. Any site with cryptanalysis puzzles will have the equivalent of this as the first challenge. Any university will also first introduce you to this (I bet even some schools teach this). It's also pretty common knowledge (the cipher which is applied here). It's actually somewhat obnoxious because it's made to appear more difficult than it actually is to someone who has either never been introduced to perhaps what is the most famous cipher or is puzzled by the abstraction that is the convolution through the application of dot codes (or unfamiliar symbols in general), thereby giving the impression the puzzle is complex when it is, in fact, the most trivial cipher to break. I find this funny because it's incredibly ironic: Kerckhoffs's principle in the form of Shannon's maxim, which states "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them," which directly contrasts "security through obscurity" by definition. The latter idea is not only strongly rejected by cryptographers in favour of the former principle — it is rejected across proper security engineering practice as a whole. This puzzle applies an abstraction as a red-herring in order to give the impression it is more difficult to break, and therefore more secure, than the actual underlying cipher at play here truly is. A hint would be that any given geometric substitution cipher is identical to any given monoalphabetic substitution cipher from a cryptanalytic standpoint. It should be obvious why this is the case. If not, what creates the distinction between a set considered alphabetic and one which is not?

This is no insult to you, OP. I just find this "problem" by the FBI laughable, almost insulting even, because they've represented the simplest cryptanalytic problem using a "dot code" (geometric substitution for the blind perhaps) to convolute the most trivially broken cipher on top of using buzzwords and mentioning "cryptanalysts" generally to create the impression that this is even worth any cryptanalysts time (skilled or not: you're not a cryptanalyst if you struggle with this at all). I would've expected something worth doing, let alone even clicking on it, being from the FBI.

If breaking crypto (while also learning crypto) is of interest to you, I would recommend checking out Matasano's crypto challenges at <https://cryptopals.com> (NCC Group acquired Matasano Security for \$13 million in 2012, but they had nothing to do with the development of these challenges and are not very crypto-oriented unlike those of Matasano, who are all-round true security experts). Thanks NCC Group, group of assholes! Set 8 will never be published. The first set that would've introduced attacks on Elliptic-Curve Cryptography and Galois/Counter Mode (GCM). Anyway, as far as cryptanalytic puzzles go (that are also useful in real-world systems), there's simply no better. You will start with implementing introductory-level cryptographic algorithms that are insecure by design, which you will then break, continually and progressively until you start building and breaking crypto-systems incorporating completely secure algorithms implemented insecurely — this is a huge takeaway. No convoluted bullshit.

Depending on whether or not you've taken computer science, or mathematics, etc., and have picked up discrete mathematics, set 5 may become the upper-bound (if not earlier: it gets challenging towards the mid-end of set 3, I would say). Plenty of modern crypto relies heavily on number-theoretic mathematics, which is a subset of discrete mathematics (core subject in computer science and overlapping courses). Prior to set 5, the mathematics is not difficult (nor is number theory once applied in cryptography (in my opinion); in fact, it's quite intuitive). The only issue you may have is if you do not know any programming. If you're an experienced programmer but would like to learn a new language and/or paradigm, I always advise people to apply it there (trust me when I say it's a great way to apply what programming [and even cryptography] theory you learn). To truly be decent, though, learning cryptography outside of that is fundamental (properly; personally, I took it at university, and it boosted the foundation Matasano brought me such that knowing crypto at that level cannot compare to the challenges [but they go amazing hand-in-hand]). These sets of puzzles, however, will get you on a very good path if you do it right (there's some hack, shitty code slapped together as "solutions" — no sense of good programming practice, logic, and most of all: patience and/or curiosity).

Faceless Man - August 8, 2019, 9:41 am

(Aug 8, 2019 09:22 AM)Phizo Wrote: [\[CITE\]](#) I'm pretty disappointed that the FBI would post such a trivial puzzle. This can be solved using introductory-level cryptanalysis; more precisely, you can solve this at not much more than a glance if you've ever done any basic cryptanalysis (the type of cryptography you break at the back of a newspaper — I'm not joking), as this simple puzzle is akin to the first (and extremely basic) cipher you would've encountered anywhere relevant to cryptography. Any site with cryptanalysis puzzles will have the equivalent of this as the first challenge. Any university will also first introduce you to this (I bet even some schools teach this). It's also pretty common knowledge (the cipher which is applied here). It's actually somewhat obnoxious because it's made to appear more difficult than it actually is to someone who has either never been introduced to perhaps what is the most famous cipher or is puzzled by the abstraction that is the convolution through the application of dot codes (or unfamiliar symbols in general), thereby giving the impression the puzzle is complex when it is, in fact, the most trivial cipher to break. I find this funny because it's incredibly ironic: Kerckhoffs's principle in the form of Shannon's maxim, which states "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them," which directly contrasts "security through obscurity" by definition. The latter idea is not only strongly rejected by cryptographers in favour of the former principle — it is rejected across proper security engineering practice as a whole. This puzzle applies an abstraction as a red-herring in order to give the impression it is more difficult to break, and therefore more secure, than the actual underlying cipher at play here truly is. A hint would be that any given geometric substitution cipher is identical to any given monoalphabetic substitution cipher from a cryptanalytic standpoint. It should be obvious why this is the case. If not, what creates the distinction between a set considered alphabetic and one which is not?

This is no insult to you, OP. I just find this "problem" by the FBI laughable, almost insulting even,

because they've represented the simplest cryptanalytic problem using a "dot code" (geometric substitution for the blind perhaps) to convolute the most trivially broken cipher on top of using buzzwords and mentioning "cryptanalysts" generally to create the impression that this is even worth any cryptanalysts time (skilled or not: you're not a cryptanalyst if you struggle with this at all). I would've expected something worth doing, let alone even clicking on it, being from the FBI.

If breaking crypto (while also learning crypto) is of interest to you, I would recommend checking out Matasano's crypto challenges at <https://cryptopals.com> (NCC Group acquired Matasano Security for \$13 million in 2012, but they had nothing to do with the development of these challenges and are not very crypto-oriented unlike those of Matasano, who are all-round true security experts). Thanks NCC Group, group of assholes! Set 8 will never be published. The first set that would've introduced attacks on Elliptic-Curve Cryptography and Galois/Counter Mode (GCM). Anyway, as far as cryptanalytic puzzles go (that are also useful in real-world systems), there's simply no better. You will start with implementing introductory-level cryptographic algorithms that are insecure by design, which you will then break, continually and progressively until you start building and breaking crypto-systems incorporating completely secure algorithms implemented insecurely — this is a huge takeaway. No convoluted bullshit.

Depending on whether or not you've taken computer science, or mathematics, etc., and have picked up discrete mathematics, set 5 may become the upper-bound (if not earlier: it gets challenging towards the mid-end of set 3, I would say). Plenty of modern crypto relies heavily on number-theoretic mathematics, which is a subset of discrete mathematics (core subject in computer science and overlapping courses). Prior to set 5, the mathematics is not difficult (nor is number theory once applied in cryptography (in my opinion); in fact, it's quite intuitive). The only issue you may have is if you do not know any programming. If you're an experienced programmer but would like to learn a new language and/or paradigm, I always advise people to apply it there (trust me when I say it's a great way to apply what programming [and even cryptography] theory you learn). To truly be decent, though, learning cryptography outside of that is fundamental (properly; personally, I took it at university, and it boosted the foundation Matasano brought me such that knowing crypto at that level cannot compare to the challenges [but they go amazing hand-in-hand]). These sets of puzzles, however, will get you on a very good path if you do it right (there's some hack, shitty code slapped together as "solutions" — no sense of good programming practice, logic, and most of all: patience and/or curiosity).

Im pretty new when it comes to Cryptography, I just started to learn recently, took me about 30 mins in total, barely ever looked at it much tbh.

But thanks for posting in the site, don't worry, once I figured it out I felt so dumb for even thinking 30 minutes total :D I've done harder ones, just thought it was interesting the FBI would post something so easy on there.

DW I don't take offence

StrikerICA - August 8, 2019, 9:59 am

datePublished": "2013-04-02T12:10:00+00:00",

Faceless Man - August 8, 2019, 10:04 am

(Aug 8, 2019 09:59 AM)StrikerICA Wrote: [CITE](#) datePublished": "2013-04-02T12:10:00+00:00",
Yeah, saw that :D lmao

rob43 - August 8, 2019, 11:41 am

Hi this is the person that was requesting a hacking service. I can't send a PM to you yet due to being a newly registered member. The discord ID is rabbitier#0655 Please delete this comment for me entering. Thanks.

