Real World Graduation: Question 80: Encryption

Edward D. Duvall
27 Apr 2019

Question 80

A certain foreign group is in the business of smuggling heroin into the U. S. They are aware that the FBI and DEA have tapped their phones and are monitoring their emails. They wish to communicate to their allies in the U. S. that: a) a shipment of 40 kg of heroin is available; b) it will brought into New Orleans, LA on the 14th of April; and c) they will meet their co-conspirators at the pre-arranged safe-house at noon. It is decided send this message by posting it on a blog using a pre-arranged user name, and using an encryption method developed by the group and their allies. Thus, even though the blog were being monitored by the FBI and the DEA, they believe a sufficiently strong code will prevent the police from figuring out what is going on.

Here are the candidate codes they have developed, each of which sends the message above:

1) `XCV TY YORE BNY EDT WSAAAW PLLU GJJ GYEWQ`
2) `B9X42 N83 FGJPT 6HOGD 9JNU 49 BPO954E VB6 R5 4E3F GA 78HB`
3) `83927 83261 90943 74835 12772 81934 61732 91846 91034 17283 81926 88225`
4) `#7(*^ %^#ED *(K 7H 9JH6& FGR^N GHE$4 GH*DE H&%%B &()UH ERBVG`

Which is the most effective way for the drug dealers to send their secret message?

a) Code #1, because it is the shortest, and hence the most efficient.
b) Code #2, because it uses numbers and letters and has no repeating sequences.
c) Code #3, because it consists only of numbers in a uniform sequence of 5 characters, which does not give any hint about what words are being represented.
d) Code #4, because it uses all the characters on the keyboard, and therefore is more difficult to break.
e) The group should use commercial encryption software.

http://edduvall.com
edward.d.duvall@gmail.com

Answer to Question 80

This is a trick question. All the answers are false. The problem with the codes developed by the drug dealers is that each of them appears to be an encrypted text. If it appears to be an encrypted text, especially a simple one that could be developed by non-experts, it will be easily broken.

As for answer e), it is likely that some government agency already has the keys for all commercial software, or has already broken it. Even if they haven't broken it, the government could get a court order to have the email decrypted by the software developer. It is likely that all data in the "cloud" is already available to most government agencies and commercial providers.

The most effective code is the code that does not appear to be a code. The best way to communicate a secret message is to convey it in such a way that camouflages the fact that it contains a secret message.

http://edduvall.com
edward.d.duvall@gmail.com