(U) What Is It Like to Do Cryptanalysis in the Year 2006?

FROM: [redacted],
Cryptanalysis Development Program Graduate
Run Date: 10/11/2006

(U//FOUO) SID today interviewed [redacted] a recent graduate of the Cryptanalysis Development Program , to find out what cryptanalysis is all about in modern times.

- ***(U) People outside the cryptanalysis career field may have seen movies and articles about Bletchley Park in the 1940's and its cryptanalysts working with pencil and paper to crack codes. They may also assume that nowadays massive banks of computers do all the work. What's the reality? What's the role of a cryptanalyst in the year 2006?***

(TS//SI//REL) The reality lies somewhere in between those extremes. Computers now perform much of the tedious work once performed manually by cryptanalysts. However, without a firm understanding of what our predecessors at Bletchley Park and similar centers were doing with their pencil and paper, even the most powerful computer is useless. Every means of cryptography is still in practice by our adversaries, from simple substitution to elliptic curve cryptography. A modern cryptanalyst must be familiar with the strengths and weaknesses of all of these techniques. Depending on the assigned task, we might find ourselves hunched over a coded message with a pencil and paper, just like in the 1940's, or we could be programming those computer banks to decipher huge amounts of collected data. Sadly, no computer can be quite as advanced as the ones shown in Hollywood fiction (sorry, " *24* " fans).

(C//SI//REL) The role of a cryptanalyst attempting to exploit intelligence can be broken into three categories:

1. *Analysis* :
   (S//SI//REL) With a seemingly limitless stream of data being collected by NSA, it must be organized and examined. Trends in the information can reveal encoding methods. Research is conducted to determine how and where the data was created. Collection systems are built to streamline the dataflow, providing the cryptanalyst with as much encrypted data as possible.

2. *Diagnosis* :
   (S//SI//REL) Using statistical, logical, and mathematical inferences, determine how the data was encrypted. This is the most challenging step of cryptanalysis, since it is much like trying to learn a new language with no translation guide. Diagnosis of a newly discovered cryptosystem can require thousands of tests and require months or even years.

3. *Exploitation* :
   (TS//SI//REL) If the encryption has a weakness, design an attack against it. In modern cryptanalysis, this usually means writing a computer program that automatically recovers an encryption key and decrypts the data. Decrypts are forwarded to intelligence analysts. Cryptanalysts working the IAD mission have an equivalently difficult job. They have to make sure that cryptography used by the NSA can resist analysis, diagnosis, and exploitation by our adversaries.

(U) Bletchley Park, the UK's codebreaking center during WWII

(U) Modern computers. (Reuters)

- ***(U) When you came to work at NSA, what did you expect your job would be***

like?

(U//FOUO) My only exposure to cryptanalysis before arriving was finishing the crypto-quote in the newspaper. On some level, I'm sure I hoped for a TV-style war room with giant computer screens and a very stressed boss yelling, "They're hacking the system!" Like many NSA positions, it is difficult to understand what the job entails until long after the job interview is over. Most incoming cryptanalysts have a faint idea of what we do by reading the description on www.nsa.gov, but that's all.

- ***(U) How has your experience so far differed from what you expected?***

(U//FOUO) Cryptanalysis isn't usually action-packed. It takes patience, hard work, curiosity, and a little luck. Every once in a while, I sit back and realize that cryptanalysts at the NSA have an opportunity to do and see things that no one else on the planet can. That makes persevering a lot easier.

- ***(U) What would you say are the most (and least) enjoyable parts of the job?***

(S//SI//REL) Every job has exciting days and dull ones. There are sometimes weeks or months spent conducting statistical tests that yield negative results. Writing a computer program to exploit an encrypted system is very tedious work. At the same time, diagnosing a cryptosystem or exploiting one of our adversary's codes gives a feeling of such accomplishment that all the tedious jobs are forgotten.