(U) Mathematician: An Insider's View

FROM: [redacted]
Diagnosis and Exploitation Support (S31153)
Run Date: 09/04/2003

(U//FOUO) What comes to mind when someone tells you he is a mathematician? ... Word problems? High school teacher? Graphing calculators? Pocket protectors? White boards filled with mile long equations? Slide rules, even? While those thoughts may be appropriate when characterizing some mathematicians, here in SID there is another dimension to the picture.

(U//FOUO) To really clear up that mental picture, you have to know that the words mathematician, cryptanalyst, and cryptomathematician are used synonymously in the field of Diagnosis. I'm a mathematician and that is my field.

(C//SI) Diagnosis is the study of cipher, enciphering key, or cryptovariables (initial key settings) in an attempt to determine the cryptographic algorithms from which they were generated. I work on the Transnational (Target) Integrated Diagnosis Focus Team. The team is made up of twelve mathematicians/cryptanalysts. Our task is to perform diagnosis on indigenous cryptographic systems and simultaneously improve the health of cryptanalytic diagnosis.

(C//SI) During the course of a normal day I run cryptanalytic routines on UNIX desktop workstations, supercomputers, and special-purpose devices using available software tools. The routines employ standard cryptanalytic tests which search for patterns and non-random properties in data. If I devise a test for which no available tools exist, then I will write software to perform the test. If I detect a significant statistical property in data, I will immediately seek, expect, and receive help from team members.

(U//FOUO) The team collaborates on diagnosis problems. It is important for me to document my test results - failures as well as successes - in our internal project news groups. It is also important for me to read the postings made by others on our news groups. The team discusses recent developments, data models, ideas, and future direction during our daily (!) team meetings.

(C//SI) On one hand, cryptanalysis can be frustrating. It is not a "do-it-yourself" endeavor. Cryptanalysts realize that the importance of achieving a successful diagnosis far exceeds the associated personal achievement. On the other hand, diagnosing a cryptographic system can prove to be a very rewarding experience. Achieving success is neither instantaneous nor deterministic. A successful diagnosis may evolve over the course of months or perhaps years. The diagnostic process may be undertaken by new cryptanalysts and it may be revisited. Sometimes taking a short step away from a problem leads to the best step forward that a mathematician will take.

SERIES:
(U) A Day in the Life of...

1. Office Manager: Jack-of-All-Trades
2. The Life of An Exec
3. Working as a Policy Analyst: One Person's Perspective
4. Data Flow Manager: The Data Fairy?
5. Mathematician: An Insider's View
6. NSA Linguists 'Panning for Gold'
7. Plenty of Action on the Action Team
8. On The Collection (Officer's) Plate
9. Sitting in the SOO's Chair
10. You Can't Keep the NSC Waiting!.. A Day in the Life of a GRSOC Analyst

without the consent of S0121 (DL sid_comms)."
