DOCID: 3929414
Approved for release by NSA on 12-01-2011, Transparency Case# 63852

[redacted] STATUTORILY EXEMPT

+----------
-------+
| THIS IS AN AUTOMATIC POSTING FROM THE ELECTRONIC SUBSCRIPTION SER
VICE.
|

+----------
-----+

Message topic:
Posted by:
This article is UNCLASSIFIED.

CRYPTOLOGIC ALMANAC
Solomon Kullback on Maintaining Communications Security

Dr. Solomon Kullback (1907-1995) was one of the "greats" in American cryptology. He was hired by William Friedman in 1930 and was part of the team that broke both the Japanese Red machine in 1935 and its successor, the Japanese Purple machine, in 1940. Red and Purple were cryptographic machine systems that the Japanese used to encipher their diplomatic messages. The breaking of these machines was a remarkable achievement because the Americans never saw them: the analysts reached their solutions solely by using cryptanalytic techniques.

During World War II, Dr. Kullback worked primarily on the solution of German systems. After the war, he was the first technical director of research and development at NSA and its predecessor agency, AFSA. He rose to the position of assistant director of research and development at NSA before he retired in 1962. Although his observations on communications security concern practices in World War II, they are still significant lessons for us today.

Attitudes are as important as actions in maintaining good communications security. Dr. Kullback believed that both the Japanese and the Germans followed some good communications security practices, but their downfall was their attitudes.

Physical security was one of the enemy's strong points. For instance, "Japanese cryptologists worked in a room that had no windows. The only entrance was through a trap door in the ceiling. German cryptologists worked in areas that were protected by a guard at the entrance holding a loaded pistol [and keeping] a police dog at his side. The Japanese and Germans erred in their attitudes by making a distinction between physical security and cryptographic security." They also emphasized physical security at the expense of cryptographic security.

STATUTORILY EXEMPT

The Japanese and the Germans had cocky attitudes. They believed that their codes were invincible or "impossible to break." As Dr. Kullback explained: "Careless mistakes by the enemy gave us the clues that enabled us to break into a wide variety of systems. By contrast, Mr. Friedman shared no such delusions. Before the Sigabas were fully operational, we received evidence that the Germans were able to read one of our codes. Changes to the system were made immediately because Mr. Friedman understood that true cryptographic security included more than just protecting the physical environment."

According to Kullback, another flaw which reduced Japanese cryptographic security was their emphasis on punishment. If anyone in a military unit admitted that he had lost or failed to destroy a code book, all of the officers in the unit above that individual would be punished along with the culprit. Consequently, soldiers would send back the cover of a code book as proof that the cryptographic material had been destroyed because it was easier to lie than to suffer the consequences. "With the assistance of the actual Japanese code books, we read messages in which an individual would brag that his military codes were destroyed."

There is substantive evidence to support Dr. Kullback's views. One of the most lucrative finds for the Allies was the entire cryptologic library of the Japanese army's 20th Division in January 1944 at Sio, New Guinea. The Japanese, who were retreating westward to Madang, did not want to be burdened carrying this material, which was in a steel trunk, over the mountains. As a result, the Ninth Infantry Division of the Australian army found the material buried near a stream bed. This capture included the additive tables, the substitution squares, and the code book itself. Since Japanese officials were told that all material had been destroyed, they did not change the system for four months, giving the Allies almost instant access to one of the Japanese mainline communication systems.

(Taken from an oral history interview with Dr. Solomon Kullback)