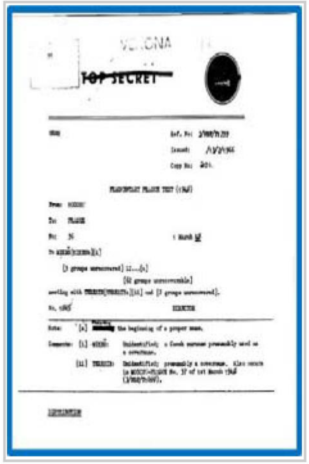
UNCLASSIFIED

DAILY ENTERPRISE

(U) HISTORY TODAY - 25 August 2015 - VENONA

FROM: CCH
Run Date(s): 08/25/2015



VENONA

~~TOP SECRET~~

[illegible]

(U) VENONA is well known today as one of the great feats of cryptanalysis. This was the last cover term for a project in which analysts discovered that a portion of Soviet messages sent from 1940 to 1948 had duplicate use of one-time pads, rendering those messages vulnerable to cryptanalysis. Once the one-time pad encipherment was stripped away, the underlying code could be attacked using traditional methods. The decrypts included messages from Soviet espionage agencies.

(U) The information resulting from this cryptanalysis changed the world.

(U) VENONA revealed that Soviet spies had penetrated the State Department, Treasury, the OSS, the Manhattan Project, the media, Hollywood, and even the White House!

(U) That VENONA was a great feat of cryptanalysis is well known. That this success was enabled by one-time pads that were mistakenly duplicated is known as well. But the fragmentary nature of the duplication is less so, and is worth explaining.

(U) One-time pads are random sequences of cipher key printed in book form. Only two copies are printed, one for the sender, one for the recipient. After a sequence of numbers is used to encipher a message, the page is destroyed. If that number sequence is never reused or repeated, the messages are unbreakable.

(U) The VENONA breakthrough was possible not, as is sometimes believed, due to Soviet code clerks lazily reusing entire pads. That would have been too easy. In reality, the error was in the original factory production of more than two copies of pad pages, undoubtedly due to wartime pressures; as the German military advanced into the Soviet Union, many factories were hastily moved east of the Ural Mountains.

(U) The fragmentary nature of VENONA was a result of irregular distribution of the duplicate pad pages; this is illustrated by the earliest message that was broken, VENONA 36, sent from Moscow to Prague on March 1, 1940. The text is as follows:

"To Mikes [Mikesh]

[3 groups unrecovered] Li...[possibly the beginning of a proper name] [62 groups unrecoverable] meeting with Terezie [Tereziya] and [2 groups unrecovered]."

(b)(3)-P.L. 86-36

[redacted]

(U) The beginning of the message, through the syllable"Li" was sent in duplicated key. The next 62 groups were not, and could not be decrypted. The rest of the text, the meeting with Terezie and two unrecovered groups, were all sent in duplicated pad again. Perhaps the Soviet code clerk used the end of one page for the start of the message, an entire page for the middle, and the start of another page for the end, and only the first and last page happened to have been duplicated.

(U) (The users were not aware that the pages had been duplicated; only a person or two in the one-time pad production facility knew this.)

(U) But the duplicate pad usage was not the whole story of the decryption. Once the one-time pad was removed, the code groups had to be decoded. Of the perhaps double-handful of groups in our example that had the one-time pad stripped off, about half never had their code values determined, and, with almost no context, were not going to be figured out from this message. A fair proportion of VENONA reads like our example, with unrecoverable portions, often quite large. Too much was not, in fact could not, be recovered.

(U) The importance of VENONA is nevertheless virtually indisputable, and the fragmentary nature should now be more clear. The luck still needs explanation.

(U) First, consider the knowledge gained from the decryption. Many espionage small fry were exposed, but the cases of three figures identified through VENONA messages show its significance: Julius Rosenberg, an electrical engineer whose contacts among government technicians enabled him to pass secrets about American advanced weaponry to the Soviets; Harry Dexter White, a senior official in the Treasury Department in a position to influence U.S. monetary and trade policy; Lauchlin Curry, a special assistant to the President, who passed on inside information about high-level policy decisions.

(U) VENONA's revelations of the scale, scope, and significance of spying were momentous. In retrospect, though, the virtual randomness of which pages of the one-time pads were duplicated leaves room for us to wonder, what if all of that world-changing information had instead been unrecoverable?

(U) Despite the importance of the decrypts it is essential to realize that the cryptanalysts were able to exploit only about five percent of the total Soviet traffic that comes under the VENONA heading.

(U) It is quite likely the extent of Soviet infiltration would have been discovered in VENONA even if chance had dictated a different distribution of duplicated key or if U.S. cryptanalysts had exploited a different five percent. There possibly would have been enough in the decrypts to identify Rosenberg and a few others, since they were the subject of multiple messages (indicating they were likely the subject of many more that we today cannot solve); White, Currie, and a lot of the small fry are much less likely, since there apparently were fewer messages about them.

(U) We cannot be sanguine that there would be enough for the many other espionage figures who were the subject of only one or a small number of messages in the VENONA traffic. In many ways, we were just lucky that we could identify them.

(U) Above all, we don't know what is in the unbroken traffic. It all might be less important than what was broken, or it might be more. Either way, we shouldn't take it for granted.

(U) Read about the Rosenberg case here.

(U) Harry Dexter White's story was in the *History Today* here.

(U) Details of Lauchlin Curry's involvement in espionage is in the *History Today* here.

(U) The (slight) involvement of a Hollywood figure was told in *History Today* here.

(b)(3)-P.L. 86-36

[redacted]

(U) To discuss historical topics with interesting folks, visit the Center for Cryptologic History's blog, *History Rocks* ("go history rocks").
(U) Have a question or comment on *History Today*? Contact us at DL cch or [redacted]

Information Owner [redacted]
Page Publisher [redacted]
Last Modified: August 17, 2015
Last Reviewed: August 17, 2015

~~DERIVED FROM: NSA/CSSM 1-52, DATED: 20180110, DECLASSIFY ON: 20430110~~
UNCLASSIFIED

(b)(3)-P.L. 86-36

[redacted]