1,

Extra copy of pages retyped from first draft. (In case they are needed.)

" "The Magic intelligence was pre-eminently important and the necessity for keeping it confidential cannot be overestimated. However, so closely held and top secret was this intelligence that it appears the fact the Japanese codes had been broken was regarded as of more importance than the information obtained from decoded traffic."

TIME says, in connection with this phase of the story of Magic during World War II:

"So priceless a possession was Magic that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, force U.S. cryptographers to start all over again."

Now I don't want to seem to over-emphasize the importance of COMINT in the Pearl Harbor affair but I think it warranted to read you what the Majority said about it in its Report. The following comes from p. 232:

"... all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

General Chamberlin, who was MacArthur's G-3 throughout the war in the Pacific, has written: "The information G-2 gave G-3 in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." I hardly need say that we can't put a dollar-and-cents value of COMINT in the saving of lives; but we can make an estimate of what COMINT meant in the way of shortening the war by two years means. I made a calculation and found that $1.00 spent for COMINT is worth $1,000 spent for other activities and materials.

In short, when our commanders had COMINT in World War II they were able to put what small forces they had at the right place, at the right time. But when the didn't have it--and this happened several times--their forces often took a beating. Later on we'll note instances of each type.

I hope I've not tried your patience by such a lengthy preface to the real substance of my talk, so let's get down to brass tacks, and since a bit of history is always useful in introducing a subject belonging to a special and not-to-well-known field, I'll begin by giving you some historical information about cryptology, which comprises two related sciences, that of cryptography, and the other of cryptanalysis. They are but opposite faces of the same coin, for progress in one inevitably leads to progress in the other.

Now, because of the secrecy or cloak of silence which officially surrounds the whole field of cryptology and especially cryptanalytics, it is obvious that authentic information with reference to the background and development of the science in foreign countries is quite sparse; and although after World War II we learned much regarding the accomplishments in this field of work by our enemies, security rules prevent my saying very much in detail about how good or bad they were in comparison with us. Suffice it to say that we looked pretty good in cryptologic affairs; together with our principal ally, Britain, we cryptologists naturally think we won the war, though others seem to have mislaid the peace somewhere.

I can only give a fairly good account of U.S. cryptologic activities up to a certain point of time, and even then I will not be able to say very much about them simply because the story is too long to give in a lecture or even a series of talks. In the course of my talk I will present a number of illustrations of

I had intended to say a few words about the decipherment of Egyptian hieroglyphic writing because it is supposed to represent the next and a great landmark in the history of cryptology. Professor Norbert Wiener, of M.I.T., in his famous book entitled Cybernetics calls that decipherment the greatest feat in the history of cryptology, but the professor is wrong. The cryptanalysis was rather simple; the difficult part was the reconstruction of the language and its grammar. I'm sorry we can't go into that now, but I do want to add that it was very fortunate that the early students of Egyptology didn't even suspect that the Egyptians also used cryptography; there were cryptographic hieroglyphics, if you can imagine such things.

There is one person I should mention before coming to the period of our Civil War. Edgar Allan Poe, in 1842 or thereabouts, kindled an interest in cryptography by his famous story of "The Gold Bug", and by some articles on cryptography in newspapers and journals of the period. For his day he was the best informed person in the U.S. on cryptologic matters.

The period of the Civil War or the "War Between the States", in U.S. history was, as a result of the invention and development of telegraphy, a period that saw the use of cryptology in a large way. Here is a picture of a cipher device used by the Confederate Army, captured at Vicksburg, one of our Museum treasures. The device is a cylinder covered with a sheet of paper bearing alphabets, the alphabets of the Vigenere table, in other words, a pointer that you could slide, and a thumb know with which you could turn the cylinder according to the key letters. You might like to know two of the keys

they used with this system and device: COMPLETE VICTORY was the first; and COME RETRIBUTION the second.

Here is a picture of a message, authentic without question, which was sent by President Lincoln to General Burnside. It's very simple. It reads this

There was one rather interesting case, in which I happened to play a minor role. In 1916-17 the Germans financed a large number of Hindus in their attempts to stir up a rebellion in India, the idea being to cause so much trouble in India that the British would be forced to withdraw troops from the Western Front to quell disturbances in India. These Hindus were negotiating for the purchase of arms and ammunition in the United States and sending them over to India. Since the U.S. was neutral, it was against our own laws to permit such undertakings against a friendly nation. So the business had to be conducted secretly and that is how cryptograms entered into the picture. Here

In all I've said thus far about our World War I crypto-communications there's been little or nothing said about our high-command ones, messages between General Pershing and Washington, for instance. I did mention the War Department Telegraph Code of 1915, which we had when we entered the war as a belligerent. It is with some sadness but also some amusement that I tell you that soon after we joined the British they told us, with as much delicacy as you may imagine the situation required, that that code wasn't at all safe. You don't have to wonder very much what the implications of such a notice meant, and I'm sure our authorities manifested no great astonishment at the time. You'll remember what I said about the British success in solving the Zimmermann Telegram which brought us into the war on their side.

Well, steps were taken right quickly to produce a new and much safer code for the War Department and high command use; also a new one for military intelligence and secret agent communications. It was also about this time that our Navy began to improve its communication secrecy by adopting a cipher which went under the curious and almost movie-like title of the NCB--the Navy Cipher Box. It was a sort of strip cipher system and I have a picture of it.

I don't know what our State Department communication security was like in those days but I have my suspicions. The long tradition of secrecy and secret diplomacy wasn't our tradition--this was distinctly a European piece of skullduggery and we had and wanted to have no part in it. Maybe we were

taken for a cryptologic ride--I don't know. That would be something for some cryptologically-minded historian to look into--if he could have access to the records, which is very doubtful.

And here is a good point at which to bring to a close this first period. We'll continue with a bit more history in the next period but it will be devoted to watching the developments in a direction opened up by inventions made about the time of World War I.