No 3 as revised

Insert for p.1

Information regarding the Codes and ciphers employed during that period has been rather sparse until quite recently, when a book entitled Turncoats, Traitors and Heroes by Col John Bakeless, AUS, was published in 1959 by Lippincott After a good many years of research Col. Bakeless brought together for the first time a good deal of authentic information on the subject and some of it is incorporated in this lecture

According to Col. Bakeless — and believe it or not I [illegible] the British commander-in-chief in America, General Gage, had no code or cipher at all, nor even a staff officer who knew how to compile or devise one; he had to appeal to the commanding general in Canada, from whom he probably obtained the simple substitution cipher which was used in 1776 by a British secret agent who — again, believe it or not — was

General Washington's own director-general
of hospitals, Dr. [redacted] Church.

General Washington had means for
secret communication from the very be-
ginning of hostilities, probably even be-
fore the fighting began at Lexington
and Concord. If the British under Gen-
eral Gage were poorly provided in this
respect, by the time Sir Henry Clinton
took over from General Howe, who
succeeded Gage, they were much

better off — they had adequate or
apparently adequate means for secret
communication.

Summary

The third lecture in this series deals with the crypto-systems employed by the British Regulars and ~~by~~ the Colonials during the period of the American Revolution. This is followed by a brief explanation of the cryptanalytic nature of the initial breaks in the solution of ~~the age-old mystery presented by~~ the ancient Egyptian hieroglyphic writing.

LECTURE 3

Continuing with our survey of cryptologic history, the period of the American Revolution, in U.S. history, is naturally of considerable interest to us and warrants more than cursory treatment. Are you astonished to learn that the systems used by the American colonial forces and by the British regulars were almost identical? You shouldn't be, because the language and backgrounds of both were identical. In one case, in fact, they used the same dictionary as a code book; something which was almost inevitable because there were so few English dictionaries available. Here's a list of the sorts of systems they used:

a. Simple, monoalphabetic substitution--easy to use and to change.

b. Monoalphabetic substitution with variants, by the use of a long key sentence. I'll show you presently an interesting example in Benjamin Franklin's system of correspondence with the elder Dumas.

c. The Vigenère cipher with repeating key.

d. Transposition ciphers of simple sorts.

e. Dictionaries employed as codebooks, with and without added encipherment. Two such were specially favored, one, Entick's New Spelling Dictionary; and the other, Bailey's English Dictionary. Here I show a couple of pages from

Insert for p. 2 (1)

REF ID: A62862

In the way more complex than simple monoalphabetic substitution ciphers, the British under Clinton's command used a system described by Bakeless in the following terms: "... a substitution cipher in which the alphabet was reversed, 'z' becoming 'a' and 'a' becoming 'z'. To restore frequency clues, the cipher changed in each line of the message, using 'y' for 'a' in the second line, 'x' for 'a' in the third, and so on. When the cipher clerk reached 'n' in the middle of the alphabet, he started

[continued over]

over again. A spy using this cipher did not have to carry [redacted] papers, since the system was so easy to remember." The alphabets of this scheme are simple reversed standard sequences

(1A)

A B C D E F G H I K L M N O P Q R S T U W X Y Z
Z Y X W U T S R Q P O N M L K I H G F E D C B A
Y X W U T S R Q P O N M L K I H G F E D C B A Z
X W U T S R Q P O N M L K I H G F E D C B A Z Y
. . . . . .
O N M L K I H G F E D C B A Z Y X W U T S R Q P

Brkzlass doesn't explain why the cipher sequences are only 12 in number — nor does the source from which he obtained the

information, a note found among the Clinton Papers REF ID: A62852 in the Library at the University of Michigan.

Babbage continues:

(2) "Clinton also used another substitution cipher, with different alphabets for the first, second and third paragraphs. Then if an American cryptanalyst should break the cipher in one paragraph, he would have to start all over in the next. As late as 1781, however Sir Henry was using one extremely clumsy substitution cipher, in which 'a' was 51,

'd' was 54, 'e' 55. Finding that 51
and 'd' was 52 I guess
(correctly) that 'b' was 52, 'c' 53. Some-
what more complex was his 'pigpen'
cipher, in which twenty-five letters of the
alphabet were placed in squares. Then
an angle alone would represent a letter,
the same angle with a dot another letter,
the same angle with two dots still an-
other. In some cases, cryptography was
used only for a few crucial words in an
otherwise clear message, a method also
favored by certain American officials."

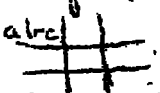
(3) Of the first cipher mentioned in the preceding extract much more to be said. Perhaps Babcock was limited by space considerations. In any case I will leave that story for another time and place. As for the second cipher Babcock mentions in the extract I can give you the whole alphabet, for it exists among the Clinton Papers:

A B C D E F G H I K L M N O P Q R S T U W X Y Z
51 52 53 54 55 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78

There is no explanation why the

(3a) sequence beginning with 50 stops with E=55 and then, starting with F=56, goes straight on without any break to Z=78. (Remember that in those days I and J were used interchangeably, as were U and V).

Finally, as to what Bakeless (and others) call the "pigpen" cipher, this is nothing but the Rosicrucian old so-called "Masonic" cipher based upon the 4-cross figure:



a = ⌟, b = ⊥, c = ⌜

which can accommodate 27 characters, not 25, as Bakeless indicates. Letters can be inserted in the design in many different arrangements.

are shown in Fig. 1.
the former. To represent a word by code equivalent you simply indicated the page number, then whether Column 1 or Column 2 contained the word you wanted, and then the number of the word in the column. Thus: The word "jacket" would be represented by 178-2-2.

f. Small, specially compiled, alphabetic 1-part codes of 600-700 items and code names; our old friend the syllabary or repertory, of hoary old age but with new dress.

g. Ordinary books, such as Blackstone's Commentaries on the Laws of England, giving the page number, the line number and the letter number in the line, to build up, letter-by-letter, by compound number, the word to be represented. Thus: 125-12-17 would indicate the 17th letter in the 12th line on page 125; it might be the letter T.

h. Secret inks.

i. Special designs or geometric figures, such as one I'll show you presently.

j. Various concealment methods, such as using hollow quills of large feathers, or hollowing out a bullet, and inserting messages written on very thin paper. Strictly speaking, however, this sort of strategem doesn't belong to the field of cryptology. But it's a good dodge, to be used in special cases.

I've mentioned that code or conventional names were used to represent the names of important persons

and places in these American colonial and British cryptograms of the Revolution. Here are ~~some~~ examples taken from a system of code names prepared by Major André, ~~of the sort of names the British used as code names:~~ the British Spy, Chief of Intelligence under General Clinton:

For American Generals - The names of the Apostles, for instance:

General Washington was "James"

General Sullivan was "Matthew"

Names of Cities	Philadelphia	- Jerusalem
	Detroit	- Alexandria
Names of Rivers and Bays	Susquehanna	- Jordan
	Delaware	- Red Sea
Miscellaneous:	Indians	- Pharisees
	Congress	- Synagogue

Insert / Names of Forts: Fort Wyoming - Sodom, Fort Pitt - Gomorrha

On Fig. 7, we see ~~Here's a very interesting slide,~~ a British cipher message of the vintage 1781. It was deciphered before finding the key, always a neat trick when or if you can do it. ~~Here's~~ the key--the title page of the then current British Army List--is shown in Fig. 8. Insert

I'm sure you've learned as school children all about the treasonable conduct of Benedict Arnold when he was incommand of the American Forces at West Point; but you probably don't know that practically all his exchanges of communications with Sir Henry Clinton, Commander of the British Forces in America, were in cipher, or in invisible inks. ~~Here's an interesting slide showing one~~ of Arnold's cipher messages, in

Insert for p 4

Fig 2a being the secret version, Fig. 2b, the plain
text. Arnold left a few words in clear, the ones
he considered unimportant; for the important
ones he used a dictionary as a codebook,
indicating the page number, column number and
line number corresponding to the position in the
dictionary of the plain-text word which the
code group represents. Arnold added 7 to
these numbers, which accounts for the fact
that first number in a code group is never
less than 8, the central number is always
either 8 or 9, and the third number is never
less than 8 or more than 36. The significant
sentence appears near the middle of the

message: " If 198.9.34 185.8 31 or 197.8.8 ..." yields the plain text: "... [illegible] but a plan of cooperation by which S.H. [Sir Henry Clinton] shall possess himself of West Point, the Garrison, etc, etc, etc, Twenty thousand pounds Sterling I think will be a cheap purchase for an object of so much importance." The signature 172.9.19 probably stands for the word "Moor"; Arnold's code name in these communications was "John Moore". He had also another name, "Gustavus".

Fig. 3 at the top shows the code message; at the bottom is the plain text. Arnold used the same additive as in the preceding example.

Insert #2 for p. 4

Insert #3 for p.4

In Fig. 4 the left-hand portion shows the "phoney" message, the right-hand one, the real message ~~To make it easy for the reader I give below in typed form both the "phoney" and the secret note, the latter being underlined.~~ Masks having small rectangular apertures etc

Explain hourglass in Cir

Insert #1 attached

which he offers to give up West Point for £20,000, is shown in Fig. 2, Figure 3 is a message ~~Here's another one~~ in which he gave the British information which might have led to the capture of his commander-in-chief, General Washington. ~~But~~ However, Washington was too smart to be ambushed--he went by a route other than the one he said he'd take.

Insert #2 attached

You may find ~~this next slide~~ Fig. 4 interesting as an example of the special sort of mask or grille used by Arnold and by the British in their negotiations with him. The real or significant text is written in lines outlined by an hour-glass figure and then dummy words are supplied to fill up the lines so that the entire letter apparently makes good sense. To read the secret message you're supposed to have the same size hour-glass figure that was used to conceal the message. The significant text in this example is ~~underlined~~:

"~~You~~ will have heard, Dr. Sir I doubt not ~~only~~ long before ~~you~~ this can have reached you that Sir W. Howe is gone from hence. The rebels imagine that he is gone to the ~~Eastward~~ Southward. However he has filled Chesapeake Bay with surprise and terror ...etc."

l c. ⊙ 1/m sp

Arnold even used the trick, mentioned above in method j, that was quite similar to one used recently

Insert for p. 5 — transferred matter from p. 3

The numbers REF ID:A62852 obviously refer to line numbers and letter numbers in the line of a key text, the first series of numbers, viz, 22.6.7.39.5.9.17, indicating line number 22, letter numbers 6.7.39.5.9.17 in that line. Because of the many repetitions the plain text was obtained by straightforward analysis by an officer presently on duty in NSA, Capt Edward W. Knapper, U.S.N., to whom I am indebted for this interesting example.

over

The plain text, once obtained gave him clues to what the key text must be, simply by replacing the plain-text letters in their numerical equivalent order in the putative key text. This done, Capt. Knapper was quick to realize what the key text was: An Army List. The date of the message enabled him to find the list without much difficulty in the Library of Congress.

Insert from page 2:

An interesting episode involving concealment
of this sort is recorded by John Bakeless.
~~in his recently published book Turncoats,~~
~~Traitors and Heroes~~: An urgent message of
Sir Henry Clinton, dated 8 October 1777,
and written on thin silk, was "concealed
in an oval silver ball, about the size of a rifle
bullet, which was "handed to Daniel Taylor,
a young officer who had been promised
promotion if he got through alive. The bullet
was made of silver, so that the spy could
swallow it without injury from corrosion.
... Almost as soon as he started, Taylor

REF ID:A62852

was captured... Realizing his peril too late, the spy fell [redacted] of terror and, crying, "I am lost" swallowed the silver bullet. Administration of a strong emetic soon produced the bullet with fatal results, for Taylor was executed. "A rather heartless American joke went around," adds Bakeless, "that Taylor had been condemned 'out of his own mouth.'"

It is often referred to as "The Benedict Arnold's Treasonable Cow Letter."

(Fig 5)

by the Russian spy, Colonel Abel, who was arrested in New York in June 1957, tried and convicted, and is still languishing in a Federal prison. ~~Here's a picture of the gentleman. How would you like to meet up with him suddenly some dark night at a secret rendezvous?~~

Insert attached

We next see (Fig. 6) one Benedict Arnold message that never was deciphered.

Only one example is extant; certain words have purely arbitrary meanings, as prearranged.

Insert matter from p. 3 here

There was an American who seems to have been the Revolution's one-man National Security Agency, for he was the one and only cryptologic expert Congress had, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages obtained in one way or another by the Americans. Of course, the chief way in which emeny messages could be obtained in those days was to capture couriers, knock them out or knock them off, and take the messages from them. This was very rough stuff, compared to getting the material by radio intercept, as we do nowadays.

I think you'll be interested to hear a bit more about that one-man NSA. His name was James Lovell and besides being a self-trained cryptologist, he was also a member of the Continental Congress. There's on record a very interesting letter which he wrote to General Nathaniel Greene, with a copy to General Washington. Here it is.

Philadelphia, Sept. 21, 1780 1/

Sir:

You once sent some papers to Congress which no one about you could decipher. Should such be the case with some you have lately forwarded I presume that the result of my pains, herewith sent, will be useful to you. I took the papers out of Congress, and I do not think it necessary to let it be known here what my success has been in the attempt. For it appears to me that the Enemy make only such changes in their Cypher, when they meet with misfortune, as makes a difference of position only to the same alphabet, and therefore if no talk of Discovery is made by us here or by your Family, you may be in chance to draw Benefit this campaign from my last Night's watching.

I am Sir with much respect.

Your Friend,

Maj. Genl. Greene
(with copy to Genl. Washington)

JAMES LOVELL

In telling you about Lovell I should add to my account of that interesting era in cryptologic history an episode I learned about only recently. When a certain message of one of the generals in command of a rather large force of Colonials came into Clinton's possession he sent it off post haste to London for

solution. Of course, Clinton knew it was going to take a lot of time for the message to get to London, be solved and returned to America--and he was naturally a bit impatient. He felt he couldn't afford to wait that long. Now it happened that in his command there were a couple of officers who fancied themselves to be cryptologists and they undertook to solve the message, a copy of which had been made before sending the original off to London. Well, they gave Sir Henry their solution and he acted upon it. The operation turned out to be a dismal failure, because the solution of the would-be-cryptanalysts happened to be quite wrong! The record doesn't say what Clinton did to those two unfortunate cryptologists when the correct solution arrived from London some weeks later. By the way, you may be interested in learning that the British operated a regularly-established cryptanalytic bureau as early as in the year 1630 and it continued to operate until the end of July 1844. Then there was no such establishment until World War I. I wish there were time to tell you some of the details of that fascinating and little known bit of British history.

There's also an episode I learned about only very recently, which is so amusing I ought to share it with you. It seems that a certain British secret

agent in America was sent a message in plain English, giving him instructions from his superior. But the poor fellow was illiterate and there wasn't anything to do but call upon the good offices of a friend to read it to him. He found such a friend, who read him his instructions. What he didn't know, however, was that the friend who'd helped him was one of General Washington's secret agents!

The next illustration (Fig. 9) is a picture of one of several syllabaries used by Thomas Jefferson. It is constructed on the so-called two-part principle which was explained in the preceding lecture. Figure 9a is a portion of the encoding section, and 9b is a portion of the decoding section, in which the code equivalents are in numerical order accompanied by their meanings as assigned them in the encoding section. This sort of system, which, as I've already explained, was quite popular in Colonial times as in the early days of Italian cryptography, is still in extensive use in some parts of the world. Jefferson was an all-around genius, and I shall have something to say about him and cryptography in a subsequent lecture.

A few minutes ago I mentioned Benjamin Franklin's cipher system, which, if used today, would be difficult to solve, especially if there were only a small amount of traffic in it. Let me show you what it was.

Franklin took a rather lengthy passage from some book in French and numbered the letters successively. These numbers then became equivalents for the same letters in a message to be sent. Because the key passage was in good French, naturally there were many variants for the letter E--in fact, there were as many as one would expect in normal plain-text French; the same applied to the other high-frequency letters such as R, N, S, I, etc. What this means, of course, is that the high-frequency letters in the plain text of any message to be enciphered could be represented by many different numbers and a solution on the basis of frequency repetitions would be very much hampered by the presence of many variant values for the same plain-text letter. As in Fig. 10 you can see this very clearly.

I know of but one case in all our U.S. history in which a resolution of Congress was put out in cryptographic form. It is shown in Fig. 11 — a resolution of the Revolutionary Congress dated 8 February 1782. I have in my collection not only a copy of the resolution but also a copy of the syllabary by which it can be deciphered.

Interest in cryptology in America seems to have died with the passing of Jefferson and Franklin. But if interest in cryptology in America wasn't very great, if it existed at all after the Revolution, this was not the case in Europe. Books on the subject were written, not by professionals, perhaps, but by learned

amateurs, and I think you will find some of them in the NSA library if you're interested in the history of the science. The next illustration (Fig. 12) is ~~Here's the frontispiece~~ of a French book the title of which ~~I translate~~ as "Counter-espionage, or keys for all secret communications correspondence." In the picture we see ~~Here's~~ Dr. Cryppy It was published in Paris in 1793. himself, and ~~this is~~ perhaps a breadboard model of a GS-11 research analyst, or maybe an early model of a WAC.

I am going to take a bit of time now to tell you something about Egyptian hieroglyphics, not only because I think that that represents the next and a great landmark in the history of cryptology, but also because the story is of general interest to any aspiring cryptologist. About 1821 a Frenchman, Champollion, startled the ~~unscholarly~~ world by beginning to publish translations of Egyptian hieroglyphics, although in the budding new field of Egyptology much had already transpired and been published. In Fig. 13 we see ~~Here's a picture of~~ the gentlemen and in Fig. 14 ~~here's~~ a picture of the great Napoleonic find that certainly facilitated and perhaps made possible the solution of the Egyptian hieroglyphic writing--the Rosetta Stone. The Rosetta Stone ~~which~~ was found in 1799 at Rashid, or, as the Europeans call it, Rosetta, a town in northern Egypt on the west bank of the Rosetta branch of the Nile. Rosetta was in the vicinity of Napoleon's operations which ended in disaster and when the peace treaty was written

Article 16 of it required that the Rosetta Stone, the significance of which was quickly understood by both the conquered French and victorious British commanders, be shipped to London, together with certain other large antiquities. The Rosetta Stone still occupies a prominent place in the important exhibits at the British Museum. The Rosetta Stone is a bi-lingual inscription, because it is in Egyptian and also Greek. The Egyptian portion consists of two parts, the upper one in hieroglyphic form, the lower one in a sort of cursive script, also in Egyptian but called "Demotic." It was soon realized that all three texts were supposed to say the same thing, of course, and since the Greek could easily be read it served as what in cryptanalysis we call a "crib." Any time you are lucky enough to find a crib it saves you hours of work. It was by means of this bi-lingual inscription that the Egyptian hieroglyphic writing was finally solved, a feat which represented the successful solution to a problem the major part of which was linguistic in character. The cryptanalytic part of the task was relatively simple. Nevertheless, I think that anyone who aspires to become a professional cryptologist should have some idea as to what that cryptanalytic feat was, a feat which some professor--but not of cryptologic science, I think it was Professor Norbert Wiener, of

the Massachusetts Institute of Technology--said was the greatest cryptanalytic feat in history. We shall see how wrong the good professor was, because I'm going to demonstrate just what the feat really amounted to by showing you some simple pictures.

First, let me remind you that the Greek text served as an excellent crib for the solution of both Egyptian texts, the hieroglyphic and the Demotic, the latter merely being the conventional abbreviated and modified form of the Hieratic character or cursive form of hieroglyphic writing that was in use in the Ptolemaic Period.

The initial step was taken by a Reverend Stephen Weston who made a translation of the Greek inscription which he read in a paper delivered before the London Society of Antiquaries in April 1802.

In 1818 Dr. Thomas Young, the physicist who first proposed the wave theory of light, compiled for the 4th volume of Encyclopedia Britannica, published in 1819, the results of his studies on the Rosetta Stone and among them there was a list of several alphabetic Egyptian characters to which, in most cases, he had assigned correct values. He was the first to grasp the idea of a phonetic principle in the Egyptian hieroglyphs and he was the first to apply it to their

decipherment. He also proved something which others had only suspected, namely, that the hieroglyphs in ovals or cartouches were royal names. But Young's name is not associated in public mind with the decipherment of Egyptian hieroglyphics--that of Champollion is very much so. Yet much of what Champollion did was based upon Young's work. Perhaps the greatest credit should go to Champollion for recognizing the major importance of an ancient language known as Coptic as a bridge that could lead to the decipherment of the Egyptian hieroglyphics. As a lad of seven he'd made up his mind that he'd solve the hieroglyphic writing and in the early years of the 19th Century he began to study Coptic. In his studies of the Rosetta Stone his knowledge of Coptic, a language the knowledge of which had never been lost, enabled him to deduce the phonetic value of many syllabic signs, and to assign correct readings to many pictorial characters, the meanings of which became known to him from the Greek text on the Stone.

The following step-by-step account of the solution is taken from a little brochure entitled The Rosetta Stone, published by the Trustees of the British Museum. It was written in 1922 by E. A. Wallis Budge and was revised in 1950. I quote:

"The method by which the greater part of the Egyptian alphabet was recovered is this: It was assumed correctly that the oval , or "cartouche" as it is called, always contained a royal name. There is only one cartouche (repeated six times with slight modifications) on the Rosetta Stone, and this was assumed to contain the name of Ptolemy, because it was certain from the Greek text that the inscription concerned a Ptolemy. It was also assumed that if the cartouche did contain the name of Ptolemy, the characters in it would have the sounds of the Greek letters, and that all together they would represent the Greek form of the name of Ptolemy. ow on the obelisk which a certain Mr. Bankes had brought from Philae there was also an inscription in two languages, Egyptian and Greek. In the Greek portion of it two royal names are mentioned, that is to say, Ptolemy and Cleopatra, and on the second face of the obelisk there are two cartouches, which occur close together, and are filled with hieroglyphs which, it was assumed, formed the Egyptian equivalents of these names. When these cartouches were compared with the cartouche on the Rosetta Stone it was found that one of them contained hieroglyphic characters that were almost identical with those which filled the cartouche on the Rosetta Stone. Thus there was good reason to believe that the cartouche on the Rosetta Stone contained the name of Ptolemy

written in hieroglyphic characters. The forms of the cartouches are as follows:

On the Rosetta Stone

On the Obelisk from Philae

In the second of these cartouches this single sign (point it out) takes the place of these three signs (point the out) at the end of the first cartouche. Now it has already been said that the name of Cleopatra was found in Greek on the Philae Obelisk, and the cartouche which was assumed to contain the Egyptian equivalent to this name appears in this form:

Taking the Cartouches which were supposed to contain the names of Ptolemy and Cleopatra from the Philae Obelisk, and numbering the signs we have:

Ptolemy, A.

Cleopatra, B.

Now we see at a glance that No. 1 in A and No. 5 are identical, and judging by their position only in the names they must represent the letter P. No. 4 in A and No. 2 in B are identical, and arguing as before from their position, they must represent the letter L. As L is the second letter in the name of Cleopatra, the sign No. 1 (point) must represent K. Now in the cartouche of Cleopatra, we know the values of Signs Nos. 1, 2 and 5, so we may write them down thus:

In the Greek form of the name of Cleopatra there are two vowels between the L and the P, and in the hieroglyphic form there are two hieroglyphs, this ~~(point)~~ and this ~~(point)~~, so we may assume that ~~this one~~ the first is E and ~~this one~~ the other is O. In some forms of the cartouche of Cleopatra, No. 7 (the hand) is replaced by a half circle, which is identical with No. 2 in A and No. 10 in B. As T follows P in the name Ptolemy, and as there is a T in the Greek form of the name of Cleopatra, we may assume that the half circle and the hand have substantially the same sound, and that that sound is T. In the Greek form of the name Cleopatra there are two a's, the positions of which agree with No. 6 and No. 9, and we may assume that the bird has the value of A. Substituting these values for the hieroglyphs in B we may write it thus:

Thomas Young noticed that these two signs E and O always followed the name of a goddess, or queen, or princess, and the other early decipherers regarded the two signs as a mere feminine termination. The only sign for which we have no phonetic equivalent is No. 8, the lens, and it is obvious that this must represent R. Inserting this value in the cartouche we have the name of Cleopatra deciphered. Applying now the values which we have learned from the cartouche of Cleopatra

to the cartouche of Ptolemy, we may write it thus:

We now see that the cartouche must be that of Ptolemy, but it is also clear that there must be contained in it many other hieroglyphs which do not form part of his name. Other forms of the cartouche of Ptolemy are found, even on the stone, the simplest of them written thus: (point out on slide) . It was therefore evident that these other signs were royal titles corresponding to those found in the Greek text on the Rosetta Stone meaning "ever-living, beloved of Ptah." Now the Greek form of the name Ptolemy, i.e. Ptolemaios, ends with S. We may assume therefore that the last sign in the simplest form of the cartouche given above has the phonetic value of S. The only hieroglyphs now doubtful are (this) and (this), and their position in the name of Ptolemy suggests that their phonetic values must be M and some vowel sound in which the I sound predominates. These values, which were arrived at by guessing and deduction, were applied by the early decipherers to other cartouches, e.g.:

Now, in No. 1, we can at once write down the values of all the signs, viz., P. I. L. A. T. R. A, which

is obviously the Greek name Philotera. In No. 2 we know only some of the hieroglyphs, and we write the cartouche thus: It was known that the running-water sign occurs in the name Berenice, and that it represents N, and that this sign is the last word of the transcript of the Greek title "Kaisaros," and therefore represents some S sound. Some of the forms of the cartouche of Cleopatra begin with (this sign), and it is clear that its phonetic value must be K. Inserting these values in the above cartouche we have:

which is clearly meant to represent the name "Alexandros," or Alexander. The position of this sign (print) shows that it represented some sound of E or A.

Well, I've showed you enough to make fairly clear what the problem was and how it was solved.

That's the way in which the initial break was made in the decipherment of Egyptian hieroglyphics, and, as you may already have gathered, the cryptanalysis was of a very simple variety. It was very fortunate that the first attacks on Egyptain hieroglyphics didn't have to deal with enciphered writing. Yes, the Egyptians also used cryptography; there are "cryptographic hieroglyphics!" Here, for instance, is an example of

Insert for p. 19

The following REETIDEA62852 a long article by Étienne Drioton in "Revue D'Egyptologie", Paris, 1933. It is entitled "Essai sur la cryptographie privée de la fin de la ~~XVIII~~ dynastie" and I quote from page 14 thereof:

"Finally, the playful tendency, already pointed out in the construction of the alphabet, appears in the orthography. Certain groups offer, when

. read as clear, a fallacious meaning:
they are intentional traps, and em-
phasize the enigmatic character of this
cryptography:

Fig. 17

insert attached

substitution. ~~That character in place of this one means "to speak."~~

Before leaving the story of Champollion's mastery of Egyptian hieroglyphic writing I think I should re-enact for you as best I can in words what he did when he felt he'd really reached the solution to the mystery. I'll preface it by recalling to you what Archimedes is alleged to have done when he solved a problem he'd been struggling with form some time. Archimedes was enjoying the pleasures of his bath and was just stepping out of the pool when the solution of the problem came to him like a flash. He was so overjoyed that he ran, naked through the streets shouting "Eureka! I've found it, I've found it." Well, likewise, when young Champollion one day had concluded he'd solved the mystery of the Egyptian hieroglyphics, he set out on a quick mile run to the building where his lawyer brother worked, stumbled into his brother's office, shouted: "Eugene, I've got it!", and flopped down to the floor in a trance where he is said to have remained immobile and completely out for five days. Don't let that sort of thing happen to you around here when and if you find the answer to a complex problem. The char force will probably sweep you up and throw you into the secret trash bin ~~for disposition by burning~~.

I shouldn't leave this brief story of the crypt-analytic phases of the solution of the Egyptian hieroglyphic writing without telling you that there remain plenty of other sorts of writings which some of you may want to try your hand at deciphering when you've learned some of the principles and procedures of the science of cryptology. A list of thus-far undeciphered writings was drawn up for me by Professor Alan C. Ross of London University in 1945 and had 19 of them. Since 1945 only two have been deciphered, Minoan Linear A and Linear B writing. The Easter Island writing is said to have very recently been solved, but I'm not sure of that. There are some, maybe just a very few, who think the hieroglyphic writing of the Ancient Maya Indians of Central America may fall soon, but don't be too sanguine about that, either.

Should any of you be persuaded to tackle any of the still undeciphered writings in the list drawn up by Professor Ross, be sure you have an authentic case of an undeciphered language before you. ~~Here's~~ Fig. 10 one that was written on a parchment, known as the Michigan Papyrus. It had baffled certain savants who had a knowledge of Egyptology who attempted to read it on the theory that it was some sort of variation--a much later modification--of Egyptian hieroglyphic writing. These old chaps gave it up as

Insert for p. 21

¶ The next period of importance in this brief account of the history of cryptology is the one which deals with the codes and ciphers used by the contestants in our Civil War, the period 1861–65. It is significant and important because, for the first time in history, rapid and secure communications on a large scale became practicable in the conduct of organized warfare

and world-wide diplomacy. They became
practicable when photography and
telegraphy were joined in happy,
sometimes contentious, but long-
lasting wedlock.

a bad job. Not too many years ago it came to the attention of a young man who knew very little about Egyptian hieroglyphics. He saw it only as a simple substitution cipher on some old language. He tackled the Michigan Papyrus on that basis and solved it. He found the language to be early Greek. And what was the purport of the writing? Well, it was a wonderful old Greek beautician's secret formulae for further beautifying lovely Greek young beauties--maybe the bathing beauties of those days.

There is one person I should mention, however, before coming to the period of the Civil War, ~~or, as some people prefer to call it, the war between the States, in U. S. history.~~ I refer here to Edgar Allan Poe, who in 1842 or thereabouts, kindled an interest in cryptography in newspapers and journals of the period, both at home and abroad. For his day he was certainly the best informed person in this country on cryptologic matters outside of the regular employees of Government departments interested in the subject, and in saying this I am assuming that cryptology was used ~~to a limited extent~~ by our Department of State for communicating with ambassadors and consuls abroad. I suppose that the Army and Navy used codes and ciphers after the Revolution but the record is a bit fragmentary and I won't be able to ~~we'll come to them a little later, when I'll show you examples of them.~~

To return to Poe, one of our early columnists, there's an incident I'd like to tell you about in connection with a challenge he printed in one of his columns, in which he offered to solve any cipher submitted by his readers. He placed some limitations on his challenge, which amounted to this--that the challenge messages should involve but a single alphabet, ~~with variants~~. In a later article Poe tells about the numerous challenge messages sent him and says: "Out of perhaps 100 ciphers altogether received, there was only one which we did not immediately succeed in resolving. This one we demonstrated to be an imposition--that is to say, we fully proved it a jargon of random characters, having no meaning whatever." I wish that cipher had been preserved for posterity, because it would be interesting to see what there was about it that warranted Poe in saying that "we fully proved it a jargon of random characters." Maybe I'm not warranted in saying of this episode that Poe reminds me of a ditty sung by a character in a play put on by some undergraduates of one of the colleges of Cambridge University in England. This character steps to the front of the stage and sings:

"I am the Master of the College,
What I don't know ain't knowledge."

Insert for p. 23

If any of you are interested sufficiently to wish to learn something about Poe's contributions to cryptology, I refer you to a very fine article by Prof W.K. Wimsatt, Jr., entitled "What Poe Knew about cryptography", Publications of the Modern Language Association of America, New York, Vol LVIII, No. 3, September 1943, pp 754-79. In it you'll find references to what I have published on the same subject.

Thus, Poe. What he couldn't solve wasn't a real cipher--a very easy out for any cryptologist up against something tough.

This completes the third lecture in this series. In the next one we shall come to that interesting period in cryptologic history in which codes and ciphers were used in this country in the War of the Rebellion, the War Between the States, the Civil War--you use your own pet designation for that terrible and costly struggle.