SCAMP 1958

LECTURE I - Section 2 - 1525 - 1615

Total No. of Slides -16



232

Butish Cipher Message resing title page of the Army hist J message dated 13 Sept 1781

٢

The New Spelling Dutionany by Rev John Entrik, London, 178 257

LECTURE

REF ID:A38382

The syllabary used by Thomas Jefferson (Extract from decoding section)

/That all 'round genius also may be regarded as being the first American inventor of cryptographic devices -- as will be discussed later.7



REF ID:A38382 631 Jefferson Sylla Encoding I of the small codes & syllabaries 1 ypres ar ted-

In addition, Code or conventional untils to rep Butish used code names In Clinton Papers following are American Generals. Apostle ladelphia. andria Detroit 12 Dolaurere Jor Phanisco ong

ID:A38382 REF LECTURE NOTE REVOLUTIONARY WAR PERIOD - Systems used by Americans and by British Americans -British iphees (a Simple monoalph sub b Monoalph with variants by use of long key sintence à ta Franklin C Vigénère with reporting key a Monoalphabetic sub b Vigeniese with repeating key C. Givilles O Entrek's a Dictionaries Bailings b Small alphabetec 1-part codes of 600-700 itema and code names c Ord book such as Black stanc-page line, no. of Words in line -odes a Dictionaries b Keybook using words c Syllabories) { Secret inks Grilles

une total Lecture I my Botroa Such 631 Total 191 63 3) 25-4) 232 5) 2321 Ł 6) 243 244 7 8 6.4 りくら 10) 6.6 67 17) 6.8 13) 69 Alfut 231 in here (Lovell letrer) 15) 240 hecture I 16 6 10 rud Sect

No slide

Revolutionary War Period - Systems used by Americans and by British:

Americans:

a

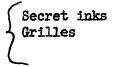
British.

- a monoalphabetic sub.
- b. Monoalph. with variants b Vigenere with repeatby use of long key ing key
 - c. Grilles

- Cuphers
- by use of long key sentence ela Franklin. c. Vigenere with repeating key

Simple monoalph. sub.

Americans: a. Dictionaries b. Keybook using words c. Syllabaries



British:

- a. Dictionaries.
 - 1. Entick's
 - 2. Bailey's
- b. Small alphabetic 1-part codes of 600-700 items and code names.
- c. Ord. book such as Blackstone - page, line, no of words in line.

-2-



AECTURE I Section 2 - 1525-1615 somin

Jotal nº . [Slidos-16

- - -

In addition, code or conventional words to represent names of persons and places. British used code names In Clinton Papers following are found:

> American Generals - Apostles (Washington = James (Sullivan = Matthew

- Philadelphia Jerusalem
- Detroit Alexandria
- Delaware Red Sea Susquehanna - Jordan
- Indians Pharisees
- Congress Synagogue

-3-

REF ID:A38382 _____6.31

Jefferson Syllabary

(Encoding) (enciphering) encrypting

Typical of the small codes and syllabaries used at the time.

The syllabary used by Thomas Jefferson (Extract from decoding section)

(That all 'round genius also may be regarded as being the first American inventor of cryptographic devices -as will be discussed later.)

h

The New Spelling Dictionary by Rev. John Entick, London, 1782.

REF ID:A38382

232

British Cipher Message using title page of the Army List. Message dated 13 September 1781.

Applies to 232.1

Line 22

GOVERNORS LIEUTENANT GOVERNORS & C OF HIS 4 5678910 17 12 15 17 17 11 23 25 21 29 31 22 33 34 36 38 1 1 1 18 20 22 24 26 28 30 35 37 MAJESTY'S

Line 23

GARRISONS AT HOME AND ABROAD, WITH THEIF ALLOWANCES

"No 6"

39 4 15-17 MEET

- 6-

REF ID:A38<u>3</u>82 2<u>32.1</u>

The key for the preceding message.

(Finding the key after solution.)

WAIT:

Before showing the next slides explain about British cryptanalysts working on American ciphers.

-7-

Franklin (Dumas) Cipher-Key Text. 1706-1790.

244

Franklin (Dumas) Cipher-Encipher Table.

Beale Papers

-8-

Benedict Arnold - "James Moore, Edward Fox, Gustavus" Major Andre - "Joseph Andrews, John Anderson"

(See next card for text.)

Arnold, disgruntled with injustices of Congress, starts off anonymous correspondence, giving information showing he is well-placed. Arnold gets command of West Point. They used secret inks; Bailey's dictionary, word cipher with words out of Blackstone and songbooks, grilles, slips of paper enclosed in specially constructed hollow bullets. Andre captured Sept 1780, writes out full confession and was hanged. Arnold barely escapted to Br. lines (peculiar part of Arnold's treason).

-9-

64

One of the cipher letters sent by Benedict Arnold to Sir Henry Clinton: 15 July 1780.

"If I point out a plan of cooperation by which S(ir) H(enry) (Clinton) shall possess himself of West Point, the garrison, etc. etc., twenty thousand pounds Sterling I think will be a cheap purchase for an object of so much importance."

(Full text - see typewritten sheet accompanying plate 6.5)

-1Ø-

REF II	C:A38382
	6.5
Plain text of the preceding message.	
Treason against Washington. Arnold lays a trap for Washington.	6.6
Another example of Benedict Arnold's ciphers	6.7
Arnold's Treasonable Cow Letter	68
-11-	

6.9

Example of a grille used by British.

231

LOVELL, James

Congress' cipher expert who managed to decipher nearly all, if not all, of British code messages intercepted by the Americans

* * * * * * * *

(To Gen Greene, cy to Wash.)

Philad Sept. 21,1780

Sir:

You once sent some papers to Congress which no one about you could decypher. Should such be the case with some you have lately forwarded I presume that the result -12-

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 in position only to the same alphabet) and therefore if no talk of Discovery is made by me 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

James Lovell

Stop - Don't click Tell about next great landmark--Egyptian Hieroglyphics and Poe.) -13-

But British cryptanalysts also were at work on American ciphers

Tell about collection of Clinton Papers at Clements Library, U. of Michigan Tell about how an operation went awry because of incorrect solution by British Army Cryptanalysts (amateur) with British Army in America

Tell about the British Ageny who was illiterate.

And about Ellis history. "The Secret Post Office and Office of Decipherer."

Enciphered resolution of the Revolutionary Congress of the U S., 8 February 1782.

6.10

Interest in cryptology in Europe.

Frontispiece of Dlandol Contre - Espion 1793.

Breadboard model of WAC or WAVE Cryptographic Officer

-15-

SCAMP 195% Lecture I of the invention and clevelop-appear devices and machines History ment of 1 July 1958 Section 2 -Section 2 2:15- 3.05 50m 3 .5 - 405 20 100 ..

REF ID: A38382 SCAMP 1958



1 July ł ŀ Cryptomachines etc Secture $\mathbf{N}_{\mathbf{A}}$ Section 1 (35 places) 2- (Ar pludes) Sect 158.1 45 452 _ 59 454 65 47 57 71 47,1 48, 172 711 49 49,1 112 49,4 71.3 495 172-1 50 72 501 165 172.2 160.1 JASX 504 159.1 172-10 170-A 502 505 1702 506 1707 507 170.9 172.4 508 172-5 5011 50.12 > 173-21 174 52 74 54 74.1 55 742 171.1 58 56 164 70.1 528 60 703 178 2601 179 260 261-A 180 261-B 182 183 262 ন্যন্থলৈ 185 186 3 1861 236 237 129 ł

130

Three or four years ago I was asked to give a lecture before the Communications - Flectronies Durision of the Air University, USAF, on the subject of communications security (COMSEC). About that fine there was being hammered into our ears over the radio of plago concerned with betomobile traffic suffyrules The plogan was "Don't learn lows by accident I thought the Alogan ful as the title of my talk but I modefiel it Dou't learn the consec Little 3 la acute y talk &

I know of course, that this group here today is not concerned particularly with COMPSEC duties of any sort. But the definition of the word Jaccident will nevertheless be of interest in connection with what will be said in a moment or two so Diel read Webster's defini-troning you'll bear with me.

Accident ferally, a An event X hat takes the one's foresult Jungxported ndeh en, a Lient. b. Hence, often, an underigned unforesan Doccurrence. J Vou affe mish or Unfortunate heracte C resulting mon damage fr as to de er dent. ٥

awing defined the word Del now ing an ent relat orontina And minor. eless Thite never ىس de of the walt w 4 ahr و re d ling duce the ær Aay

3 During the war, the President of the United States. Commander-in-Chief-of-the-Army-and-the Navy, the Chief of Staff of the Army, the Commander-in-Chief of the U.S. Fleets, and certain other high officers of Government journeyed several times half-way around the world to attend special meetings and conferences. They apparently could go with safety almost anywhere exceptdirectly-across or over-enemy or enemy-occupied territory -they met with no "accident". On the other hand, the Japanese Commander-in-Chief of the Combined Fleet, Admiral Isoroku Yamamoto, the man who was maligned by erroneously attributing to him a 10/1 statement to the effect that he was "looking forward to dictating peace torms in the Khate House", (he actually said something of quite different import, viz, that in embarking on a war with the U.S. the Japanece would have to viewalize

that its end could come only if they could distate peace terms in the Winte House), went on an inspection trip in April 1943, the sequel to which may be summarised by an official Japanese Navy Department communique reading in part as follows

"The Commander in Chief of the Combined Fleet, Admiral Isoroku Yamamoto, died an heroic death in April of this year, in air combat with the enemy while directing operations from a forward position." 4. As a file the case, the communicated didn't while the while truth. "Yamamoto didn't die "in air combat with the enemy while directing operations" - he met with an "accident". I don't combined the vivid description, but it's decidedly applicable in this case "accidents don't happen-they was brought about!" Our Navy communication intelligence people were reading the Japanese

REF ID:A38382 a ρ ¢-NO. ~ đ٦ 00

l(

232,1 The key for the precedury message [Funding the key after polition] Wait | Beforz Showing next two plides explain about Butsch Cryptandyte working on Am. ciphers.

ID: A38382 REF 243 Manklen (Dumes) Cipher - Key Text

REF ID: A38382 Franklin (Dumas) Cepher-Encipher Table



no slide

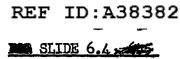
LECTURE NOTE

\$

See next eard for =

Benedict Arnold -"James Moore, Edward Fox, Gustavus" Major Andre -"Joseph Andrews, John Anderson"

Arnold, disgruntled with injustices of Congress, start off anonymous correspondence, giving information showin he is well-placed. Arnold gets command of West Point. They used secret inks; Bailey's dictionary; word ciphen with words out of Blackstone and songbooks, grilles; slips of paper enclosed in specially constructed hollobullets. Andre captured Sep 1780, writes out full con fession and was hanged. Arnold barely escaped to Br. lines (peculiar part of Arnold's treason)



LECTURE

One of the cipher letters sent by Benedict Arnold to Sir Henry Clinton:- 15 July 1780

"If I point out a plan of cooperation by which S(ir) H(enry) (Clinton) shall possess himself of West Point, the garrison, etc. etc, twenty thousand pounds Sterling I think will be a cheap purchase for an object of so much importance."

(For full text see typewritten sheet accompanying plate 6.5.)

REF ID:A38382 65 Plan text of the preceding message

REF ID:A38<u>3</u>82 -6.6

LECTURE NOTE

Treason against Washington. Arnold lays a trap for Washington.



D:A38382 1) Austher example of Benedict 6.7 Arnold's uphers D 3) Armold's Treasonable Cowletter 6.8 3) Example of a golle used by British 6.9

REF ID:A38382 6.8 The Bandet Arnold Indecipherable Cow Jetter

REF ID:A38382 69 Example of grille message (British)

LECTURE NOTE

LOVELL, James

Congress' cipher expert who managed to decipher nearly all, if not all, of British code messages intercepted by the Americans."

 J
 k. -}
 ** * * * * * *
 *

 J
 k. -}
 -1-.
 Philad.
 Sep. 21, 1780

 Sir:
 1
 -1-.
 Philad.
 Sep. 21, 1780

You once sent some papers to Congress which no one about you could decypher. 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 (OVER)

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 in position only to the same alphabet and therefore if no talk of Discovery is made by me 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

REF ID:A38382 no slide

But British cryptanalysts also were at work on American ciphers -

(Extract from Ellis history here.)

Jell about alloction of Cluston Papers at Clamento Library, U J. Mich fell about n ope lesausa the Omo

Wart! And tell about the Butch agent who was illiferate. And about Ellis history "The Secret Postoffere and Office of Desigherer"

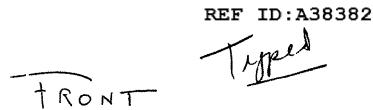
ID:A38382 REF Encycheted resolution of the Revolutionary Congress of the US 8 Feb 1982

Interest in cryptology in Furspe la 10 1) Frontrepiece of Dlandol Contre-Espion 1793 2) Breadboard model of WAG or WAVE Cryptographic Africer

Dlandol frontispiece (a cryptographer at work)

His assistant -- early model WAF





Southwes I, III

_REF_ID:A38382

SCAMP 1958 INECTURE I - 24 June 1958 28 studes Section 1 - 12/15 - 1510 55 minutes 16 " " 2 - 1525 - 16\$5 50 " 105 . 44



-

LECTURE I - Section 1 - 29 June

1. appreciate opportunity be participant of SCAMP '58 and to talk a bit about Som the interesting etusodes an unportant ndmarks that stand out in t he hestorecal background of the par art I crypt - morting me to speak on එ හි he elizer we 21 backhr /L cr. marily to do will Which has ment and uner l' linplay ary

3. Now aughtology has cartainly not always been considered a vital military weapon, or even as a weapon. For instance even as recently as in 1955, when the U.S. was fying to shalp our most unportantally in the Eulitwation of the cryptologic goodens by providing has with the money for the se Amentioned sust a Rent moments -gd, we pought to Use funds allocated mal Defende Assistance MJAP-TRO (Must Pact. But those funds are specifically commarked for research and developism

REF ID:A38382 physical water ments, machines, bened hopelass even to try to the use of MDAP money followy research and development of only after we had the formation wash in which military crypt Heogy been used in World War I and the funds sought were gr 4. This point about cryptology be useful duly for such Felatwelly unent portent ends Das personal diarias love

REF ID:A38382 messives, and altempts to prove that Baron of somebody else wrote the plan remends haborber which mare ry of the old Persian Queen Someut 5. The Seme Sto

3

Stay, weary traveller!

If thou art footsore, hungry, or in need of money -Unlock the riddle of the cipher graven below-And you will be led to riches beyond all dreams of avarice!

0, thou vile and insatiable monster! To disturb these poor bones!

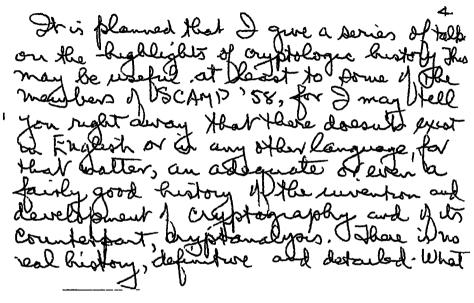
If thou had'st learned something more useful than th art of deciphering,

Thou would'st not be footsore, hungry, or in need of money!

Many times during course of last 30 years I've had occasion to wish I knew the old gal's present address so that I could put as a 1st Ind. to her basic communication the single word "Concur"

A-1 1. Appreciate opportunity to talk to students and faculty of Electronics Division of Air & Mmand and Staff School of USAF Air Unive sity 2. In inviting me to speak on subject "Communications Intelligence" it was indicated that "the objective is to create an awareness of the background. development and manner of employment of this vital military weapon. 3. COMINT not always regarded as "vital" or meven as a "weapon". Story of Semiramis (over) (Well, anyhow it's been an interesting life!) -Bead-axtracts Scon THE of 17 Dog / Extracts from B. H. report (noxt card)

D



its and proces one funds have and there law accoults are generally ful in popu of misunderstandings mis 1 down bit light Of coupe Office is a good reson wh no history of cryptology worky of the name had been produced for four use It is that as a rule abovernments don't publish tham or portinit its ergoto logic workers to publish histories brochurs or articles. This is an understandable and sensible rule of not carried to abound

TD • 238382

and illegreal limits by monstring that all 5 COMINT thust be perfet secret for all time Fater on I may tell you about an amisin I not enlightending conference I was a silmmoned to acted at the Pantagona week ago today. Of course , mow and then some cryptblogre information does lack out, so for example, holen congressional and other official investigations either require or additably the desclosure

TD:A38382 REF of such information, or when some formal filipted worker commits indescriptions in Consciously and deliberately breakothe ust that Rod been imposed . I Cf both these types of security breaches I officed in personal - Q shall have more to say later on. AV The moment of pullmerely comment that the bistory which cours from such leapages and breaches of thust are apply to contain crocors, I mounderstandings, destrictions, and less

may have wondered what 6 talk or serves of talks is the tills to fell y me u could be 50 Land Art ~~) 300 Alice . te mysell. 4K2 leved to stat low desclose m that the + to, Dom June V all be Ar here who day the delession the latones un and SCAMP are US. Navy. proper that I the suddenly gone

unagune I'm Admiral Mahan, I has a anglain tent the "C" in the "title of alk is not the work "SEA" but the letter "C" and it stanks for the word GRYPTOLOGIC The type of the talk is harefore 'The influence of chyptologic power on history " Asla Dul befor this, "Or about to wow boattles and white and go down in history as a great tactician, strategist and leader of men or, on the other thand, how to love -battles and wars and go down in history

REF ID:A38382 as an masm der. a heel, a'no-good-nik? U. rler me bant At this bo en to den how I'm Casting any reflec certain successful Apeltacularly Cessful commandars - Buch as Joher Fisethover and mac Arthur. Bu Thanks well, occur to you without my sail here to your a Adultan -Q.J.D here (Il be warnes of man in sach of the a calagous t'how to wind a love hables and was

ਸਤਕ ID:A38382 + Fin remended) montgomer and I have イン d ant i fo re monty in للاهن group such as thus a acesahr to make endut but Ble wake . QQ - Instorians know that the histor of deblowary and wanfare feams with Justs where the furn of effects was gee

affected by the relative cryptologic power of the opposing forces. Most of the history in the history books, when first written, does not tell the complete story or the whole truth -- for the cryptologic facts centuries, or maybe never (Tell about (1) Minason (Scinut Elist), (2) Mary Up Research on Battle Aflanhe, (3) Wayser Behire of Sometimes the course of history is materially or drastically changed by the existence of COMINT, or it could have been changed by its proper use -- as some say about the COMINT available to us before Pearl Harbor; but sometimes, also, the course of history is materially changed by the non-existence of COMINT where it had previously existed and was used. We discuss an unitary the later type too in due court first, an unident of the former type - fragely the former type

My talk will be divided into three sections, and the title contended Section is: "The influence of C - power on history."

Lest there be some in my audience who may fear that I have forgotten I am speaking at the Air Um versity and not at the Naval War College, I besten to say that I am not laboring under the allucination that I am Admirel Mahan, or Mahan's ghoss; where the "C" in the title of this section of my talk stands for "Cryptologic" - "The influence of Cryptologic Power on history." Not the history of mankind and particularly of warfare teems with instances where the turn of events was much (OVER)

usone of O 194 least V-E an days rea. the part of vociferous Kepu clamor on lecaus. disclosing to the world. The upon learning and a been caught by purprise disastrons we ha Garome h wolficted upon us at B papenese. earl emor to_ when no longer be hushed by the need for So there restrations My Decreen , the

٢ ~ ~ J ል 5 11 Sear than S. L. Jas ĸ ustall - the al 3-920-0 . Vin Oslevi. MARKE IL ما \sim 464 J. ha 46.2 Jac. 'SEA'GH the CPY PTELOGIC The К., k. s.

ID:A38382 REF only itself brought into the open every 82 detail and bacheout in its own langt investigation and hearings but also Thisclosed everything that was said and shown at all the provides Army and Nary uvestigations - about a tall dogu re came a day in the Congressing carmon when General Herge C Marshall buel of Statt, US, Army at the Henre Holdend Harlos uttack, was Edlad to the watness stand He testifical for soveral days, forg Ling ones: Toward the Quel of the ordeal J

reved about a latter of had the was quest been undered had written to Governor Deven in the autumn of 1944, devin the Prepadentral Campand acuser (Marshall Balked He toleafed most corn. when with the Committee not to pretime to detectore the later or its content, but to no avail He had to ton to the will the Committee Read TIME to Uneary Secret

A lew ago I to The Do Ege Ul ry il gets by مە ALD abl to low X1.... ndusp, disto mi • a on Dian And this allo 3 14 sharp of them where cu in bai C: This TIME deput, comment these of the onaval tet marol the SI were نمدا letter which had been prepared low Marshell's who got the result CA ~~~ ory pito V was An Staller

lot me ______ nout 4 m ۵ TANEX È.

REF ID:A38382 on who followed at all ٨U closures -the hable an sures from the point of view of the fourt all on Parl Harbo red or been mustified by 75 we were really read The Or Barl Harth, why wer wey Caught by Pour the alter ৸৶ ٤U سالمله all men ten Couple 1 3000 do an those by battleships in harbo all. this blanes on the groun ---to these heets Majority of, reposite Con

REF ID:A38382 Pag & Narooty Report (20 July 1946): INTELLIGENCE AVAILABLE IN WASHINGTON (M "With the grance -- et "With P, The Con

REF ID:A38382 win later to the Marshall - Dewey corres. mane "MAGIC" a meant by the - How did the terms come to be used ? It was introduced into our usage by the It was the cover name during the WW I years 1 the product 1 COMINT operates how carefull IC - even the fac a very Slewler three or its continuance Only a very few 1. for instance - Marshell Dawey th wachine OSS in heabon in

the det that ۵J YEar of ю ~ Q., nD at all 11570 0

REF ID:A38382 bout Fearl Harbor. 86 ener persons who shell argue about Eveny so offen the story هين are Vranned aa Trovers of 160 (A redarchard at RANNIS still wor langthy trantice on the Aubject lit-wagers are of course, still conversed and ane toware other Americans that President Sendet brought the attack about and deliberated me if them atake phocking charges and alloged Constancy gunony Roosevelt Stark & Which & Coulde is nonsense. by rether easy, lo maybe Jee go But now tots

REF ID: A38382 (87) The harm that the dischoors if then letter caused to our national Sectrety is incalculable The trainings were lipen and the documents (40 vokemes) are public decuments. Should we be greatly astomoted that contain governments have greatly Declurity devices and unrangements sure the close of the Congrassional.

read now from p 232 of the Mayout Report Athe Joint Congressional Committee ... all wetnesses familiar with Magic material . Throughout the war have testified that it contributed enormously to the defect of the avery great eved the war, and Saved many thousands of kurjas - Beveral Chamberton (9-3 of gen machthurs staff throughout the war in the lacifier) Atold we (The put শ -7 group brig Tubater alone scarted us man photened the warby no bas the I handly need say what the On They so made a callculation + found that \$100 spent for COMINT = \$1000 spent for other

WWII when we had have COMMY EN, our pike in our struggle against two very despe the Ster ut was de Japanese, It the suffer had marie not what fitte we had at the regult time in the next And when we deduct have it - as in the fathere - alinot terribly descotions Battle of the Bul we Ra mi icter -Bhy from - well, aug sond, When we dide have it ming went body because our principal J-25 had come to sky too bearts on よ The Battled the Bulge down astelle · Read

ID:A38382 REF 1 Show 1st page of Baldwin article (Sell 2. Fada prom next card - Merson 3. Hen read extracts from \$ 40

1

9) (947) -Z155 Jur. Extract from: Merriam, Robert E., Dark December; The full account of the Battle of the Bulge, p. 211:

"According to Eisenhower's personnel officer, American losses in the Battle of the Bulge totalled 76,890 men, of whom 8,607 were killed, 47,139 wounded, and 21,144 missing. Over 8,000 of these casualties were in the 106th Division. Because of heavy German attacks, 733 tanks and tank destroyers were lost. Two divisions, the 28th and 106th, were nearly completely annihilated, although the 28th Division did subsequently enter combat after being rebuilt."

10 have sie not tored you out by such a ley face to the real substatuce of my Which came first - secret writing ? Ur plain-text writing ? The art of winding probably grew out of pictographic and its growth can be traced back to the down of ewil yed man Rebuses

REF ID:A38382 229 marshall - Dewey photo

REF ID:A38382 4.1%

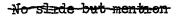
Example of rabus (pr)-

REF ID:A38382 Cryptanalysis - and psychoanalysi, -in the Bible.

Nebuchadnessar and his dream Jamil Chapter 2 3, 4, 5, 6, 7, 8, 9, 1011 Delshaggar - 11 5: 1-5, 25-30

Cupherde

TD:A38382 Read from Bible - Daniel MENE, MENE, TEKEL SUPHARSING BELSHAZZAR of "The Handwriting on the wall" DANIEL The First Cryptonalyst (BE 570-569) "______Second Psychoanalyst or interpreter Instances of actual eight in the Bible : Jeremiah 25, 26 51, H





Instances of cipher in the Bible

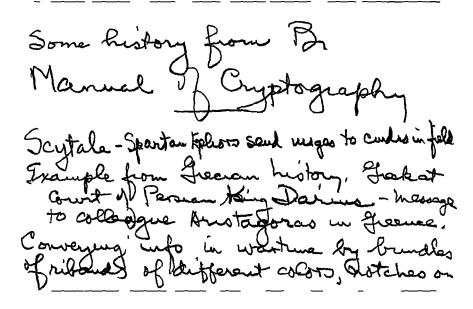
Jeremiah 25.26 51:41

Scylale

REF ID:A38382 え

Scytale

Wait - see next card



stak buts ted in varous ways - Fires or beacons -all nations of antique Politus describes system used by freeks-Conditionate mystern - the dwilled water of 5 and the num ber 1 pro lit separate places davoted the group of + the position of the letter in that group. Fires as Rate as 1746 in Staby to Sug code given to general the Marquis de Mireto worked cortes Fr Stort Idenese my of drums - only chiefs if tubes

EF-ID: <u>A3838</u> Caesar's cipher - invented, many Canturies earlier en various countries by Calthagenians + Phoenicians Used by Germans in 1870-71 + by Bor forces during S. African war

The only suptems known to have been employed between time of Julius Caesar + the bedrining of the 16th Coutling are two:) gaventicly it. d=: e= ... 0= ... U=:... Eth: t::wn c:pit::I:t:d system in which' consonants remain in altered but the vowels are replaced by the immediately following consonant of 2) System in which co

REF ID:A38382 For many centuries after Roman invo selmost supral reglested and enson being that the art of sever writing an hoven was long redarded as Forle One Here are many ustances of students of it being acculated of sorcering among whym may le mentored Trithemen 1 Spankern. 6 - B 10 Of Crystoghaph 10 also en Courty, spe Henry IV (1553-1610) + chiefs

D:A38382 3.1 RUNES on a stone in front of Gripsholim-Castle near Stockholm A.S Rune - a secret, a mystery". "Maigue". Any of the characters of the alphabet formarking w dendral use by the Tentome, or Germanic, peoples from about the 3d Century A.D. Blocked net portion - enother type of "Ruin"

Deginnings of mod p of modern cryptology can & rack to the days of the early للهو raced & the 15th utry years of inplayed by t Qri atès apal 4 chancernes abet 21401! For example, see alpe [next shile]

REF_ID:A38382 4.10 Cipher apphabet of 1401

, these ama But herently detail the um 11 80-1

REF ID:A38382 کی

SCYTALE

245,2-

Tpukiennes 1518 Abbe' of Spanheum

REF ID:A38<u>3</u>82 151

Trithemian Oath

Present oath

Back up by P. L. 513 - now 18 USC 798

We administer a special oath to everybody who comes into the field -

Back it up with

PUBLIC LAW 513 now 18 USC 798 1st Slide



REF ID:A38382 246 . 3 Framples of uplar applabates and small Clabouries used centures ago, (1) Charlemegne's cipher (768-814) 2) Arter Cycler used in England during per (34) 3) Ugam writing I anerest Eve 4) Ogam-like alphabet of Charles I (1646) to Marques. 5) Marques of Worcesters "Clock Cipber" (3) Curdhnal UW alsey, 1529, Vienna Smith Pars, 1863 Ser Thomas Chaloner, Madred, 1561 9) Ser Edward Stafford, Madrid, 1586

ID:A38382 REF 3.3 apher alphabet in Sir Thomas mores Utopia, 1518

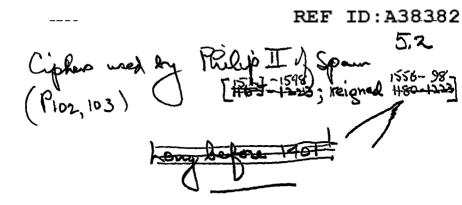
REF ID: A38382 Facundo Jacipher found Just 35 among the papers J. Mary Aucen of Scoto (1542 01587)

Queen Mangat B Cipher alph oher ta 3.7 Slut simle to the later years of Elizabeth's reign 38 The Two-word Square Cypler State explos in Churlas I's Une (1627) 201 CS with France and Flankers (AC Emphan 1510 3.9 Part of Duke of Buckengloan's capter 3.11 terneton-F precionation for communea 1 Septis ତ used in Neron . 3 10 upert and the Earl of Archugton, See State Foreign Office Cipler during relign 2 George III 311 1779

Frontroprese of "The Bebrugton Plo Celan Gordon Smith, London 19 Ciph ريک Fabrugton 11/ ce N Forger ٦



REF ID:A38382 218 Cyclers involved in the Balangton Plat The forged protocrupt



But monocliphabeter explore shell used forlay 1 3,4 Under Rumuch Spy case

REF ID:A38382 Porta's table (1563)

REF ID:A38382 61 Portais table an it appears in an early Elizabethan State paper

REF ID:A38382 Vigenère Square as pictured -

REF ID:A38382 Vigenère Square as V. describes it in his book 1586 5.1

REF ID:-A38382 104 Les used by Jalileo (1564-1642) Italian astronomer & physicist fryghene (1629-1695) O Dutch Math, physicist, & astronomer Ciphers

TD: A38382 REF One of earliest instances of the advantage On the course of Hultary gained Hornhows the capture and public queen poly Doage part by the succeed toole pla 626 h Realmout four towald hanguedoe, t 202 in possession of the Neguenots Ulul ypesieged br Ne King's hotple under com and d Vince deConde. Jater Tobout to parse preae papiel read للحثي ر woned there to surrende

REF ID:A38382 End of 1st paction Lecture I 2.15 to 3.10 = 55 minutes

agest they knew the day and they that Yamamoto would leave Truk, the time he would arrive at Buka and leave Buka for Kahilli or Ballale, what his escort would be and so on. It was relatively easy to bring about the "accident". Our Commander-in-Chief journeyed with safety because the communications connected with the was various trips were secure; the Japanese Commander-in-Chief journeyed in peril because the communications were insecure. Whis death way no ancident in the dictionary Sunse of that word, it was brought about. -I will close this introductory comment by noting that the Yamomoto "accident" is an excellent example of highly effective beauwork between the Navy and the Army Air Force in World War II. In this particular case the Navy obtained the intelligence and set the brap; the Army Arr Force sprang it.

REF A38382 5. The Yamamoto rucedant later gave rese to a somewhat amusing exchange of top secret telegrams between Tokyo and Washington, and after the war was all over these telegrams twined up in The Forrestal Diaries, Chapter III, pp 56-57

CÀRD 1

Extract from the "Forrestal Diaries," Chapter III, "Foretaste of the Cold War," pp. 86 and 87.

The formal surrender took place on the deck of the U.S.S. Missouri in Tokyo Bay on September 2. The mood of sudden relief from long and breaking tension is exemplified by an amusing exchange a few days later of "Urgent: Top Secret" telegrams which Forrestal put into his diary. In the enthusiasm of victory someone let out the story of how, in 1943, Admiral Isoroku Yamamoto, the Japanese naval commander-in-chief and architect of the Pearl Harbor attack, had been intercepted and shot down in flames as a result of the American ability to read the Japanese codes. It was the first public revelation (OVER)

of the work of the cryptanalytic divisions, and it brought an anguished cable from the intelligence unit already engaged at Yokohama in the interrogation of Japanese naval officers: "Yamamoto story in this morning's paper has placed our activities in very difficult position. Having meticulously concealed our special knowledge we now become ridiculous." They were even then questioning the Japanese officer who had been responsible for these codes, and he was hinting that in face of this disclosure he would have to commit suicide. The cable continued: "This officer is giving us valuable information on Japanese crypto systems and channels and we do not want him or any of our other promising prospects to commit suicide until after next week when we expect to have milked them dry. . . ."

(CONTINUED ON CARD 2)

Extract from the "Forrestal Diaries" continued. CARD 2

Washington answered with an "Operational Priority: Top Secret" dispatch: "Your lineal position on the list of those who are embarrassed by the Yamamoto story is five thousand six hundred ninety two. All of the people over whose dead bodies the story was going to be published have been burned. All possible schemes to localiz: the damage have been considered but none appears workable. Suggest that only course for you is to deny knowledge of the story and say you do not understand how such a fantastic tale could have been invented. This might keep your friend happy until suicide time next week, which is about all that can be expected. . . ."

w W State

Т

İ.

Extract from the "Forrestal Diaries," Chapter III, "Foretaste of the Cold War," pp. 86 and 87.

The formal surrender took place on the deck of the U.S.S. Missouri in Tokyo Bay on September 2. The mood of sudden relief from long and breaking tension is exemplified by an amusing exchange a few days later of "Urgent: Top Secret" telegrams which Forrestal put into his dary. In the enthusiasm of victory someone let out the story of how, in 1943. Admiral Isoroku Yamamoto, the Japanese naval commander-in-chief and architect of the Pearl Harbor attack, had been intercepted and shot down in flames as a result of the American ability to read the Japanese codes. It was the first public revelation of the work of the cryptanalytic divisions, and it brought an anguished cable from the intelligence unit already engaged at Yokohana in the interrogation of Japanese naval officers: "Yamamoto story in this morning's paper has placed our activities in very difficult position. Having motioulously concoaled our special knowledge we now become ridiculous." They were even then questioning the Japanese officer who had been responsible for these codes, and he was hinting that in face of this disclosure he would have to commit suicide. The cable continued; "This officer is giving us valuable information on Japanese crypto systems and channels and we do not want him or any of our other promising prospects to commit suicide until after next week when we expect to have milked them dry . . . "

Washington enswered with an "Operational Priority: Top Secret" dispatch: "Your lineal position on the list of those who are embarrassed by the Yamamoto story is five thousand six hundred ninety two. All of the people over whose dead bodnes the story was going to be published have been buried. All possible schemes to localize the damage have been considered but none appears workable. Suggest that only course for you is to deny knowledge of the story and say you do not understand how such a fantastic tale could have been invented. This might keep your friend happy until suicide time next week, which is about all that can be expected. . . ."

TD: A38382 But not many years passed before the Japanese began to realize what had happened to in the cryptologic battles of World War II. U For example: [Next two cards]

"Rear Admiral Tomekich Nomura, the last CNC in the Japanese Navy, said:

'... Not only have we been beaten in the decisive battles of this war but also we lost the communications war. We felt foolishly secure and failed to take adequate measures to protect our own communications on one hand while on the other hand we failed to succeed in breaking into the enemy's traffic. This is undoubtedly one of the major reasons for our losing battles, and in turn one one of the major contributing factors to the loss of the war. We failed in communications."

" ... Our Navy was being defeated in the battle of radio waves. Our cards were bad, and the enemy could read our hand. No wonder we could not win in this poker game!"

YOKOI, Toshiyuki - The Story of the Japanese Naval Black Chamber.

Į

A38382 Books recently put m مف Japan in nava h. + auto A come o her 24.4 1) this afeinento lefeat to poor COMSED on their salt and excellent COMINI on from Mideway book

Lest you infer that our pide didn't meet with any COMSEC "accidents," let me pay that we had plenty -but these were dot athibutable to pertins weaknesses in our COMSEC dences, machines, aufpules but to human failure to follow the rules implicitly, or - and this shorts in ou contact weaknessed in the Saying I'm t CONSEC darrees, machines, and rules of A of our alles. U Take for instance, the heavy losses the U.S Army Dir Corps sustained in their

RFF ID: A38382 air strikes on the Ploaste oil fields in southeastern Europe We lost deveral fundred big Bombers Decause of weakness we deduit radiese existed in Russhan Communications. Those big raids constatuted field days for the German figliter commands I because merely by the work, and simple at that, they I of Knew gradly when and where our bombers were booked! When we found out, it was too late! This incident leads me to pay.

ID:A38382 REF that the COMSEC weaknesses of our) leads alless and friends even today The rather selious illness which afflicts rour high - lavel or from time authorit for anon the desease a } * Achisophrey when one is your Haro. desite to continue to an over الت مەمر **ム**ァ、 he crund Stow A0. not. R -800.

TD: A38382 REF Thus far, no real as Bean la he had <u>, ko</u> LOCOMSEC m puppressed COMINT wishes. you will renderstand that this oblew is a pather periors one in certain of our allies in NATO. I may dd that UUS, and UK physics COLLA sata very claral. n Do x Fle and an astron

A38382 Joday we are going to see some plides which will illustrated important milestones in the history of the whenton and dovelopment of Deplan devices, cipher machines, ceptier appartitus, and of there is time, rules for establishing and mandaming COMSEC. The need for these things afose as a consequence of the constally meressue recessity for more socurity in military and uplomatic commencations, more lyperally after the odvent of telegraph, calle, and Natio communications subsequent to the discoveries

ID: A383 REF of the proneers in the field of electrical inventor If soon became obvious that the so-called pencil and paper cipber piptens - and a little lester, the so-colled "hand-operated" cipber devices - had to give way Ho machines and mechanical, mechanico - electrical, and now, to electronic machines As mechanization untomation progresses in civolezation, similar progress has to follow in communications, aspecially in military, haval, air, and deplomatic communi-Chifrons.

LECTURE

FOR SLIDE 45

The earliest picture of a cipher disk, from Alberti <u>Trattati in cifra</u>, Rome, c. 1470

"Oldest tract on cryptography the world now possesses"



REF ID: A38382 45 2 The Myer disk, partented 14 Nov 1865

-

LECTURE NOTE

REF ID:A38382 FOR SLIDE 45.4

The Alberti Disk reincarnated in the U.S. Army

Cupher Disk of 1914-18.



Somebody once said that the very nice looking document with paal and red ribbon the is Jussued when the US, Patent Office grants a patent is nothing but a fine looking montation to partipate in a lawsmit for influngement But the person being hurt By infungement upon his patent must be above to fle the put - or at least bus have and absorption should be alive I hout have a that Alberts or his hairs and/or assigned

were alive to contest this patent, usued in 1924, for a cipher disk practically dente with Alberti's deske if 1470'

FOR SLIDE 47

The cipher disk as again patented in 1924 -- Huntington Patent

/Shows that the Patent Office does not have general information on cryptography because of the secrecy involved./



LECTURE

REF ID:A38382 471 Cypher disk used by Nazis in 1936

REF ID:A38382 FOR SLIDE 48

Original Wheatstone cipher device (invented and describe in 1879) // Infortant /First improvement on the Alberti disk/) have one here [Show A.]



REF ID:A38382 FOR SLIDE 49

The Modified Wheatstone cipher device

/Froduced by the British Army 1917-18 but never used because of solution by Wm. F. Friedman --story of solution./



REF ID:A38382 FOR SLIDE 49.1

The Decius Wadwworth cipher device (invented and built in 1817 when Colonel Decius Wadsworth was Chief of Ordnance.)



-- --

LECTURE

FOR SLIDE 49.4

The Bazeries cryptographe cylindrique (1901) as shown in his book "Les chiffres secrets devoiles"

/But he may have described this in his article "Cryptograph a 20 rondelles-alphabets" Comptes rendus, Marselles, 1891/



REF ID:A38382 مرجد

Bozerver, Étranne

-- --

LECTURE NOTE

FOR SLIDE 50

Tust

Second page of Jefferson's description of "The Wheel Cipher"



REF ID:A38382 50 1 Second page of Sefferson's description showing his calculation of the number of permutations afforded

ID:A38382 REF Original model of Hitt's stup Explor ("The Star Eigher"). 160 2

REF ID:A38382 FOR SLIDE 50.4

Parker Hitt's model of strip cipher (1916)

Story of solution at Riverbank Laboratories of test messages prepared by Mrs. Hitt.



ID:A38382 REF Ile first six messe geo of their Plan texts of Manbergne's set of 25 challenge messages 159.1

LECTURE NOTE

REF ID:A38382 FOR SLIDE 50.2

U.S. Army Capher Device M-94.



D:A38382 Early altempts to use cylindrical Cipher device principle but with Variable alphabets (M-136) (M-137) (M-137) 50.6 (M 138-TI) 507 (M-138) 50.8

REF ID:A38382 FOR SLIDE 50.12

U.S. Army cipher device, Type M-138-A (with Russian legends)

<u>/Story of Russian legends and how they came to be there</u>

1) European model 1 stup eigher 51 2) "disabsembled 52 Syko ship cipher Pourt awards £35,000 to "mentor"

- REF -ID:A38382

LECTURE NOTE

54

The Kryha cipher machine

f.



LECTURE

FOR SLIDE 55

A German mathematical dissertation on the Kryha

/Merely number of permutations and combinations a given machine affords like - has nothing to do with the case or at least not much. Depends on nature of permutations and combinations, what they are <u>cryptographically</u>. For instance, the principle of monoglphabetic subsitution as in Gold Bug -26! cipher alphabets or the large number:-403,291,461,126,605,635,584,000,000 See over for quad/trillions/billionsmillions See over for thousand willion years to do the major part of writing these alphabets out --scroll would reach from earth peyond the planet Mercury!

73)

ID:A38382 REF 26 ! Four hundred and three quadrullions; two hundred mety-one thousand, four tundred and party one fulleois, Que hundred twenty - size 'thousand, six tundred and five billious, Sy hundred thirty - five thousand five hundred and sugar and a frew. Etop Dail diele Hustory 1/ voter

• 2383 All the preceding examples of cryptographic and one in the category of what may be thermad "pencel and paper" or I "hand-sperated" aids. These that of course, had to give way to more rapid and more secure means for crypto-communications, and this meant machines of one sort or another. - 2002r -

A38382 There was pressing need in the military and naval services for two machines 1) A small machine for low peblon or field use 2) A larger machine for read echelon and high-command use Jets take up the first of these two pes. Types.

REF ID:A38382 ۱٬۲(۱ <u>۴)۹ هد ۱٬۲۱</u>

LECTURE

M-161: Signal Corps model made at Fort Monmouth (Efforts to develop <u>field</u> machinest tell story re offuse durector of S.C Falts. Note power source



REF ID:A38382 FOR SLIDE 164

Boris C.W. Hagelin

Does a "hysteron-proteron" in inventing C-367



LECTURE NOTE

REF ID:A38382 70.1

Converter M-209



Example of American resourcefulness and skill under difficulties. Two GI's in Italy mechanize the M-209.

(The cartoon, showing a couple of GI's with a home-made "still", and the legend: "Yess, but will it work?")



ID:A38382 RFF 260.1 Hagelin CX-52 youble -ape-pri ley - h wa Inequilar Alept non guaranteed Hepping cg le

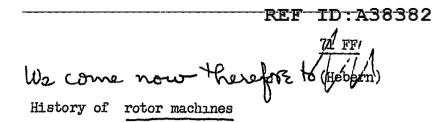
REF ID:A38382 260 Hagelin CX-52 [and its fundamental weakness] next card

ID: A38382 The big problem on the use of devices and machines which are of Deg-generator or additure (or subtractor) fype is the fact that When the alphabets worder are known alphabets, solution of a depth of two is generally possible.

RFF

D: <u>A3838</u>2 261 · A Example of Solution of polyaphabete excepterment with book-key and prown alphabets, in this case reversed standard 261-B Continuation

REF ID:A38382 262 Hagelin (M-209) Solution. "A depth of two" Stop! Dovid cleck! next card We come them to the po-called Notor mæchenes, which are not bosed upon key-gevorator principles but are permutation mæchenes



REF ID:A38382 FOR SLIDE 58.1

The Swedish electrical machine B-21

/Original Aktiebolaget Cryptographe B-21. Mention Boris C.W. Hagelin/



Swedish machine connected to electric typewriter.



REF ID:A38382 FOR SLIDE 65

The keyboard electrically-operated B-211 Swedish machine

Zelf-contained, instead of separate typewriter,7



REF ID:A38382 FOR SLIDE 57

The original (commercial) Enigma cipher machine

 \angle Later used with one improvement by Germans in World War II



LECTURE NOTE 71 Come now to american developments

Edward H. Hebern

How he became interested bography and invented Ciphen



REF ID:A38382 FOR SLIDE SHER 172

The first Hebern machine

Manufactured for use by the Ku Klux Klan7



TD: 138382 The first Hebern printing model Still a one-potor machine! 71 1 Where did he get the idea of Cascading rotors?

ID:A38382 REF 712 Hebern potors - variable 713 wiring possibilities! 13 to one pide & 13 to other

3-rotor Hebern

REF ID: A38382 71 Hebern Edward H. [How he came to intrent machine]

REF ID:A38382 LECTURE FOR SLIDE 72 165 The 5-rotor Hebern machine Istory of solution on next place 165 Tell ~

REF ID:A38382 1722 First Hebern machine built in accordance with Nary Specifi-Catrois

REF ID:A38382 172.X Hebern model SIS folved on challenge by Navy



FOR SLIDE 172.10

One of Hebern's developments for the Navy, after his release. Solenoid spiraled disign Kub successive to Navy spice

(This is the one that wouldn't work - but Hebern said the contract didn't specifically state that it had to work. He insisted on being paid -- and was!/ If was last get be did for Navy (Que havy file weisted that Navy had an admiral on havy District Had in S.F. first to beep H out 4 fail so be could finch Navy contract!) Short Touch Click . No.2 - cord 1st!

REF TD: A38382 Navy has enough of Hebern and goes in for its own development 15 years later Hebern Co. & hers withtute peut in U.S. Court of Claims for \$50,000 000 Probable settlement by nord for few probable settlement by nord for few probable settlement by nord for few

LECTURE NOTE

Collaboration and cooperation between the Army and Navy on cryptographic research and development notable for its absence in those days. Each service had its secrets!



LECTURE NOTE 170 Å

U.S. Army Converter M-134-TL

Basic principle - external keying



REF ID: A38382 170.2

Converter M 134 Rear view

REF ID:A38382 ויקס,ך

Converter M 134 with printing !

REF ID:A38382 170.9

-

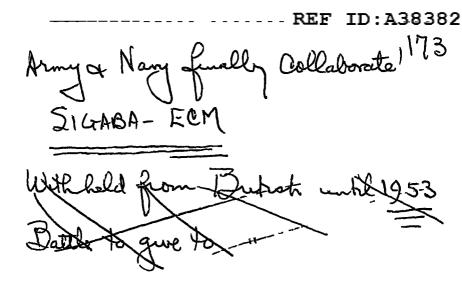
U.S. Army Converter M-134-A



_

2EE ID-13838282 1724 Original Nary Marke I ECM With Bourden weres! And only 15 starting points !

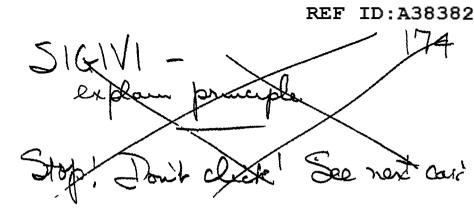
REF ID: A38382 172,5 First production model D. Nary Mark I



REF ID:A38382 174 SIGIVI or BASKET

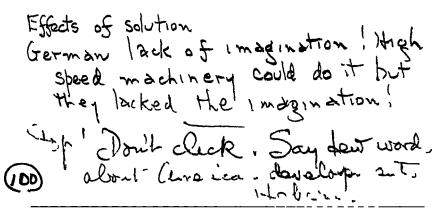
SIGABA-ECM with held from Birtroch. Battle to guve to British 1953 Finally given in 1953 But during WWII had to nudicate - the CCM

4



REF ID: A38382 $\{\frac{14}{74.2}\}$

The German Armed Forces cipher machine of WW II



REF ID: A38382 Engna S-wheel printing 58 Captured in 1945 at Mitelfels A failure !

REF _ID; A38382





German Naval Enigma differences between it + Any & Aur Force E

LECTURE NOTE



With growth of teletype communications the need for and practicability of automatic encipherment became obvious. -- The first attempt -- the machine developed by the AT&T Co. (1918) in collaboration with the Signal Corps.



LECTURE

The AT&T Co. printing telegraph cipher machine (1918) (The original SIGTOT!,) /Story of solution/



REF ID:A38382 Ex Order 25 Aug 45 Put in prequence in prefece 1 Pearl H account-introducti 10

- - -

1. Appreciate opportunity be participant of SCAMP '58 and to talk a bit about some of the interesting episodes and important landmarks that stand out in the historical background of the science and/or art of cryptology.

2. In inviting me to speak on the subject I assume that the objective is to deal with that area of the background of cryptology which has primarily to do with its development and manner of employment as a <u>vital</u> military weapon.

3. Now cryptology has certainly not <u>always</u> been considered a vital military weapon, or even as a <u>weapon</u> For instance, even as recently as in 1955,

- - - - -

when the U.S. was trying to help our most important ally in the cultivation of the cryptologic gardens by providinher with the money for the purpose I mentioned just a few moments ago, we sought to use funds allocated to MDAPthe Mutual Defense Assistance Pact. But those funds are specifically earmarked for research and development of physical instruments, machines, guns, electronic devices, etc., and it seemed hopeless even to try to justify the use of MDAP money for cryptanalytic research and development. It was only after we had pointed out the ways in which military cryptology had been used in World War I and II that the funds sought were granted.

4. This point about cryptology being useful only for such relatively unimportant things as personal

-2-

diaries, love missives, and attempts to prove that Bacon or somebody else wrote the Shakespeare Plays reminds me of a story which may be a bit apochraphyl but is somewhat amusing.

5. The story of the old Persian Queen Semiramis.

Stay, weary traveller!

If thou art footsore, hungry, or in need of money-Unlock the riddle of the cipher graven below-And you will be led to riches beyond all dreams of avarice!

-3-

0, thou vile and insatiable monster! To disturb these poor bones!

- If thou had'st learned something more useful than the art of deciphering,
- Thou would'st not be footsore, hungry, or in need of money!

Many times during the course of the last 40 years I've had occasion to wish I knew the old gal's present address so that I could put as a 1st Ind. to her basic communication the single word "Concur".

It is planned that I give a series of talks on the highlights of cryptologic history. This may be useful at least to some of the members of SCAMP '58, for I may tell you right away that there doesn't exist in English

or in any other language, for that matter, an adequate or even a fairly good history of the invention and development of cryptography and of its counterpart, cryptanalysis. There is no real history, definitive and detailed. What bits and pieces one finds here and there in popular accounts are generally full of misunderstandings, mis-statements, and downright lies.

Ł

Of course, there is a good reason why no history of cryptology worthy of the name has been produced for public use. It is that as a rule governments don't publish them or permit its cryptologic workers to publish histories, brochures, or articles. This is an understandable and sensible rule if not carried to absurd and illogical limits by insisting that all COMINT must be kept secret for all time. Later on I may tell you -5-

about an amusing if not enlightening conference I was summoned to attend at the Pentagon a week ago today.

Of course, now and then some cryptologic information does leak out, as for example, when congressional and other official investigations either require or accidently bring about the disclosure of such information, or when some formerly trusted worker comits indiscretions, or consciously and deliberately breaks the trust that had been imposed. Of both these types of security breaches-official or personal--I shall have more to say later on. At the moment I will merely comment that the history which comes from such leakages and breaches of trust are apt to contain errors, misunderstandings, distortions, and lies.

-6-

Some of you may have wondered what the title of my talk or series of talks is. Bean Swift asked me yesterday to tell him so that it could be indicated on the announcement sheet. I told him I preferred to state the title myself and I'll now disclose my secret by telling you that the title is:

"The Influence of C-power on History."

Lest there be some here who think I'm laboring under the delusion that this building and SCAMP are U.S. Navy property or that I've suddenly gone psychotic and imagine I'm Admiral Mahan, I hasten to explain that the "C" in the title of my talk is not the word "SEA" but the letter "C" and it stands for the word <u>CRYPTOLOGIC</u>. The title of the talk is therefore "The influence of -7-

cryptologic power on history." As a subtitle I offer this: "Or how to win battles and wars and go down in history as a great tactician, strategist and leader of men; or, on the other hand, how to lose battles and wars and go down in history as an incompetent commander, a heel a 'no-good-nik' "

At this point let me hasten to deny that I'm casting any reflections upon certain successful--spectacularly successful commanders--such as Generals Eisenhower and MacArthur. But names will occur to you without my calling them to your attention--and there will be names of men in each of the two categories--"how to win" and "how to lose" battles and wars.

-8-

At this point I'm reminded of a story about General Montgomery-- "Monty" and I have the story on pretty good authority.

Story re Monty in N. Africa, 1942.

Before a group such as this I think it hardly necessary to make this general statement but I'll make it. That not all historians know that the history of diplomacy and warfare teems with instances where the turn of events was greatly affected by the relative ryptologic power of the opposing forces. Most of the istory in the history books, especially when first ritten, does not tell the complete story or the whole ruth -- for the cryptologic facts are usually very arefully hidden from historians, even from official

-9-

historians, and are not brought to light for years, decades, centuries, and maybe never. (Tell about (1) Morison (Samuel Eliot), (2) Navy Op. Research on Battle of Atlantic, (3) Wenger lecture at Naval War College.

Sometimes the course of history is materially or drastically changed by the existence of COMINT, or it could have been changed by its proper use--as some say about the COMINT available to us before Pearl Harbor, but ometimes, also, the course of history is materially hanged by the non-existence of COMINT where it had "eviously existed and was used. We will discuss an neident of the latter type, too, in due course. But irst, an incident of the former type--Pearl Harbor. The tory of P.H., which I begin by reading from the 17 Dec 945 issue of TIME. I should preface the reading by

-10-

reminding you that the war was over--or at least V-E and V-J days had been celebrated -- and the clamor on the part of vociferous Republicans, who had for years been insisting upon learning and disclosing to the world the reasons why we had been caught by surprise in such a disastrous defeat and calamity as the Japanese had inflicted upon us at Pearl, this clamor had to be met. It could no longer be hushed by the need for military secrecy. So there were investigations -- a half dozen or more, winding up in a grand finale of the Joint Congressional Investigation into the Attack on Pearl Harbor It was this investigation which not only itself brought into the open every detail and exhibit in its own lengthy investigation and hearings but also disclosed everything that was said and shown at all the previous Army and Navy investigations -- about a half

--- REF ID: A38382

dozen of them.

_ _ _ _

There came a day in the Congressional Hearings when General George C. Marshall, Chief of Staff, U.S. Army at the time of the Pearl Harbor Attack, was called to the witness stand. He testified for several days, long, long ones. Toward the end of the ordeal he was questioned about a letter it had been rumored he'd written to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. General Marshall balked. He pleaded most earnestly with the Committee not to force him to disclose the letter or its contents, but to no avail. He had to bow to the will of the Committee.

Read TIME to "Uneasy Secret"

-12-

A few moments ago I commented that the sort of cryptologic history which gets published as a result of official investigations is apt to contain errors, misunderstandings. distortions. and downright lies. And this account in TIME contains its share of them. But the curious part of this story is that TIME didn't commit these offenses; they were in the original Marshall-Dewey letter, which had been prepared by somebody on Marshall's staff who got the results of COMINT but was no technician or cryptologist. I will interrupt the reading of the letter to remark that undoubtedly those of you who followed at all closely the disclosures -the remarkable and shocking disclosures from the point of view of national security--of the Joint Congressional Investigation of the Attach on Pearl Harbor must have wondered about or been mystified by this question: If -13-

we were really reading the Japanese code long before Pearl Harbor, why were we caught by surprise when the attack came? Why did we lose over 3,000 men in a couple of hours, all those big battleships in harbor, and all a those planes on the ground?

You weren't alone in thinking about this mystery. Listen to these extracts from the Report of the Majority of that Joint Congressional Committee, p. 170 & 253.

I'll return later to the Marshall-Dewey correspondence But now:

> What was meant by the name "MAGIC"? How did the term come to be used? It was introduced into our usage by the British. It was the cover name during the WW II years for -14-

for the product of COMINT operations and activities.
(1) Special intelligence, (2) Traffic intelligence,
(3) Weather intelligence.

I suppose its hardly necessary for me to tell you how carefully guarded were the fruits of the MAGIC--even the fact of its existence was known to only a very few persons. Hearings p. 261. Success--rather its continuance--rested upon a very slender thread.

Midway, for instance, Marshall Dewey letter. (J. Red machine. OSS in Lisbon. Marshall Dewey ltr.)

There are many persons who still argue about certain questions about Pearl Harbor Every so often the story -15-

comes up and the fires of controversy are fanned once again to the blazing point. (A researcher at RAND is still working on a rather lengthy treatise on the subject.) The right-wingers are, of course, still convinced and are trying to convince other Americans that President Roosevelt brought the attack about and deliberately. Some of them make shocking charges and allegations of conspiracy among Roosevelt, Marshall and Stark. Which of course is nonsense--disprovable by rather easy logic Maybe I'll go into this later if you wish.

But let's get back to the Marshall-Dewey letter.

The harm that the disclosure of this letter caused a halculable. The hearings were open and the documents

(40 volumes) are public documents.

Should we be greatly astonished that certain governments have greatly improved their communications security devices and arrangements since the close of the Congressional Investigation????

I read now from p. 232 of the Majority Report of the Joint Congressional Committee.

1. ". . . 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."

2. General Chamberlin (G-3 of Gen. MacArthur's staff throughout the war in the Pacific (told me (and he -17-

put it in writing for me on request): "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."

3. I hardly need say what the latter saving alone was worth in billions of dollars. I made a calculation and found that \$1.00 spent for COMINT equals \$1,000 spent for other war materials and activities.

Now let's see what happened during WW II when we had nd didn't have COMINT on our side.

In our struggle against two very desperate enemies, he Germans and the Japanese, it was often the possession f COMINT, the so-called "MAGIC" which meant the -18-

difference between defeat and success. When we had magic we could put what little we had at the right time in the right place. And when we didn't have it--as in the famous and almost terribly disastrous Battle of the Bulge we took a bad beating.

- READ from letter -

When we didn't have it--well, as I said, things went badly because our principal G-2's had come to rely too heavily on it.

> The Battle of the Bulge. Baldwin Article - Read.

1. Show 1st page of Baldwin article. (p. $3\emptyset$) and ead title of. -19-

_REF_ID;A38382

- 2. Read from next card __ Merriam.
- 3. Then read extracts from p. 40.

-2Ø-

Extract from: Merriam, Robert E., <u>Dark December</u>: The full account of the Battle of the Bulge, 1947-Ziff-Davis Publishing Co., p. 211:

"According to Eisenhower's personnel officer, American losses in the Battle of the Bulge totalled 75,890 men, of whom 8,607 were killed, 47,139 wounded, and 21, 144 missing. Over 8,000 of these casualties were in the 106th Division. Because of heavy German attacks, 733 tanks and tank destroyers were lost. Two divisions, the 28th and 106th, were nearly completely annihilated, although the 28th Division did subsequently enter combat after being rebuilt."

-21-

I hope I've not tired you out by such a lengthy preface to the real substance of my talks. So we'll begin by asking:

How old is the science of cryptology?

Which came first -- secret writing?

Or plain-text writing?

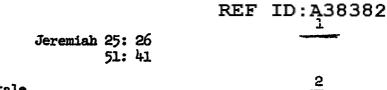
The art of writing probably grew out of pictographs and its growth can be traced back to the dawn of civilized man. <u>Rebuses</u>.

-22-

Example of rebus. (p 2)

4.12

REF ID:A38382 Cryptanalysis - and psychoanalysis -- in the Bible. Nebuchadnezzar and his dream. Daniel, Chapter 2: 3, 4, 5, 6, 7, 8, 9, 10, 11. Belshazzar - Daniel, Chapter 5: 1-5, 25-30. Read from Bible - Daniel. MENE, MENE, TEKEL (UPHARS IN (PERES Belshazzar and "The Handwriting on the Wall". Daniel - The first cryptanalyst (B.C 570-569) The Second Psychoanalyst or interpreter of dreams. Joseph was 1st. Instances of actual cipher in the Bible:



Scytale

Some history from Br Manual of Cryptography.

Scytale - Spartan Ephors send messages to commanders in field. Example from Grecian history. Greek at Court of Persian King Darius--message to colleague Aristagoras in Greece.

Conveying info in wartume by bundles of ribands of different colors, notches on stick, knots tied in various ways. Fires or beacons--all nations of antiquity.

Polypuis describes system used by Greeks--co-ordinate

system -- Letters divided into groups of five and the number of fires lit in two separate places denoted the group of letters and the position of the letter in that group. Fires as late as 1746 in Italy to signal, code given to General the Marquis de Mirepoux in command mixed corps French, Spanish and Genoese troops, still in existence.

In Africa--beating of drums--only chiefs of tribes and headman initiated.

Caesar's cipher - invented and used many centuries earlier in various countries--by Carthagenians and Phoenicians. Used by Germans in 1870-71 and by British forces during S. African war.

-25-

__ _ _ _ _ _ _ .

The only systems known to have been employed between time of Julius Caesar and the beginning of the 16th Century are two:

l. i = . a = : e = :. o = :: u = :.:
Th:. t::wn c:p.t:.:l:t:.d

2. System in which consonants remain unaltered but the vowels are replaced by the immediately following consonant.

For many centuries after Roman invasion Br crypt almost entirely neglected, one reason being that the art of secret writing was long regarded as an invention of the Evil One. There are many instances of students of it being accused of sorcery, among whom may be mentioned Trithemius the Abbe of Spanheim . . .

p. 6 - Br Manual of Cryptography. Read.

Viete - Then about him. P. 6 Br Man.

Correspondence between Court of Spain Henri IV (1553-1610) and Chiefs Anti-Royalists in France.

3.1 RUNES on a stone in front of Gripsholm Castle near Stockholm.

A.S. "Rune" - "a secret, a mystery." "Magic".

Any of the characters of the alphabet formerly in general use by the Teutonic, or Germanic, peoples from about the 3d Century A.D.

-27-

Blocked out portion -- another type of "Ruin"

151

Beginnings of <u>modern</u> cryptology can be traced back to the days of the early years of the 15th Century, when it was extensively employed by the princes and chancerrie of the Papal States.

For example, see this alphabet of 1401! (Next slide) (Cipher alphabet of 1401) Trithemuis - 1518 Abbe of Spanheim

Trithemian Oath

Present oath. Back up by P.L. 513 - now 18 USC 798 -28

We administer a special oath to everybody who comes into the field.

Examples of cipher alphabets and small syllabaries used centuries ago. (246 or 3)

- 1. Charlemagne's cipher (768-814)
 2. Cipher used in England during reign of Alfred the Great 871-901.
 (246 3. Ogam writing of ancient Eire.
 4. Ogam-like alphabet of Charles I (1646) to Marquis of Worcester.
 5. Marquis of Worcester's "Clock Cipher".
 6. Cardinal Wolsey, 1524, Vienna.

Sir Thomas Smith, Paris, 1563.
 Sir Thomas Chaloner, Madrid, 1561.
 Sir Edward Stafford, Madrid, 1586.

Cipher alphabet in Sir Thomas More's Utopia, 1518

Facsimile of a cipher found among the papers of Mary Stuart, Queen of Scots (1542-1587).

Cipher alphabet - Queen Mary Stuart and Bishop of Glasgow, then her Ambassador or solicitor in France, 1571.

Sliding-card cipher. Facsimile of one used in the later years of Elizabeth's reign (about 1600). -30-

The two-word square cipher. State cipher used in Charles'I's time (1627) for communicating with France and Flanders. (A co-ordinate system)

Part of Duke of Buckingham's cipher used in 1627 for communicating with France.

Numerical cipher used in reign of Charles II (1630-1685) between Prince Rupert and the Earl of Arlington, Sec. State.

oreign Office Cipher during reign of George III. (1779) -31-

217

218

Frontispiece of "The Babington Plot" by Alan Gordon Smith, London 1936. The cipher used by Mary Stuart Queen of Scots with Babington. (1542-1587)

Frontispiece of "The Babington Plot" by Smith The Forged Postscript, with Phillips' endorsement. (Ciphers involved in the Babington Plot. The forged postscript.)

Ciphers used by Philip II of Spain (1527-1598) reigned 1556-98. (pp. 102, 102)

-32-

REF ID: A38382 But monoalphabetic ciphers still used today' Gustav Rumrich spy case. Porta's table (1563) Porta's table as it appears in an early Elizabethan State paper.

Vigenere Square as pictured in the ordinary literature.

-33-

REF ID: A38382 Vigenere Square as V. describes it in his book 5.1(1586) Ciphers used by Galileo (1564-1642) Italian astronomer and physicist Huyghens (1629-1695) Dutch mathematicians, physicist and astronomer.

-34-

P9 - Br Manual

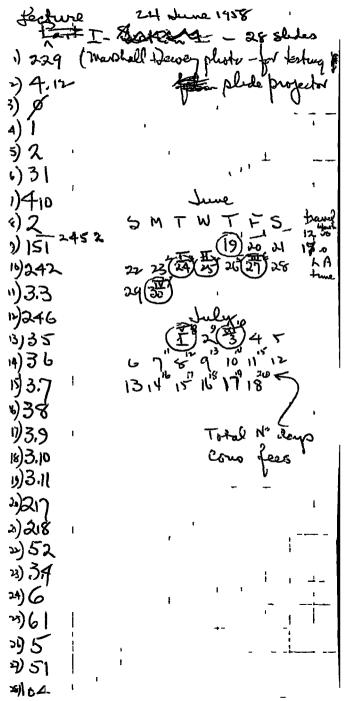
One of the earliest instances of the advantage gained in the course of military operations by the capture and subsequent solution of a message sent by the enemy took place in 1626, Siege of Realmont, a town of Languedoc, then in possession of the Huguenots but besieged by the King's troops under command of the Princ de Conde.

Latter about to raise siege. Message intercepted. Rossignol reads. Out of powder and would have to surren der if not immediately received new supply.

-35-

REF ID:A38382 <u>SCAMP 1958</u>

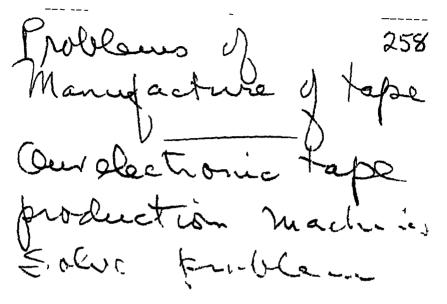
LECTURE I - SECTION 1 - 24 June 1958

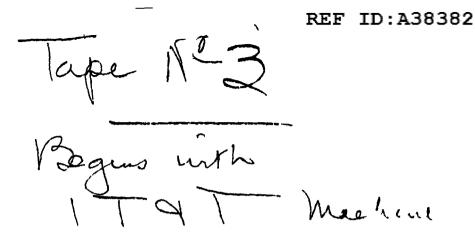


Cryptanalysis is a game, in which one's adversary makes all the rules, and moreover does his utmost to make them as complicated as possible. Consequently, though the cryptanalyst may (and should) use scientific methods in his research he cannot always be carried along by the scientist's simple faith in the fundamental rationality and uniformity of nature. He will seldom, that is, he able to solve a cypher by direct application of real mathematics, though he will often use methods which are very similar to mathematics, but lack the simplicity and elegance of the real thing and are usually much more laborious.

2. A former member of this organisation had a motto which he used to quote to new recruits "indexing is the mother of solution." When you are confronted with a pile of messages in an unknown cypher the first step, then, is to index them and see what you have got. Then you proceed to theorise about a possible solution that would account for all the phenomena recorded in your index and test it - if it fails you then think of another.

Extract from The Modern Problem .X Joshua A Cooper in remarks made on the occasion of the opening of Effegy ar GCHQ 24 Feb 1958





LECTURE

REF ID:A38382

- -

FOR SLIDE 60

The IT&T Co. teletype cipher attachment

١

/With the growth of teletype communications, cipher teletypewriter attachments were invented./

١





LECTURE NOTE

FOR SLIDE 180

SIGCUM with B-131 set and teletype machine

(SIGHUAD - aform of SIGCUM with one-time key features) (Dangers of electrical radiation) (Dangers of depth)

Stop! Ficult duck hert can!



Ł



REF ID:A38382 しゃん

Warture development Lots of brigo"

SIGMEN CIFAX

REF

ID:A38382 (Ƙ-3

ID: A38382 REF 185 CIPHONY SIGJIP- Bellelistder

REF ID:A38382

Nebern Co Sugt for \$50,000,000 Tusthuled about 10 years/ago. Probably will be settled for spent throusand

REF ID:A38382 1864 Cephony and cifax marhines 186.1 SigsALY Vocoder types

ID:A38382 REF New developments in cipher machines AFSAM - 7 AFSAM-9 AFSAM-15 -AFSAM-36 + AFSAM-Dai "Integrated" equipments Ciphony --- + its problems. Sugsal

REF ID:A38382



REF ID:A38382

ís 7 fers ٨ h <u>م</u>درا ų "+ 111 he Do. 5 n U Lag NI.

ID:A38382 REF 236 hunder of cryptographie Systems in effect 7 Dec 1941 - October 1945 [U.S. Army & Army Dir Forces only =]

ID:A38382 REF 237 number of holders of Cupptographic materials Dec 1941 - Oct 1945 [U.S. Army & Army Air Forces mey!] Stop! Don't click ! next 2 cards

ID:A38382 REF Keeping track if nateral crypto ount ٩ Japanese incident of Certif to destruction by butning

REF ID:A38382

I will bring thestalk to a close ow by repeating the importance the plogan we try to mendicate: Don't learn your COMSEC laws

REF ID:A38382 SCA MP 1950 History of the Lecture V .

REF ID:A38382 Applies to 2321 Whe 22 THE GOVERNORS LIEUTENANT COVERNORS 123 45678910, 12 13, 15167 18 920 21 22 23, 27, 27, 28, 28, 31 4-C OF HIS MAJESTT'S 32 33 3435 363738 39 4041 72434445 Ab Line 23 GARRISONS AT HOME AND ABROAD, WITH THEIR ALLOWANCES 33332 33 34 35 34 31 38 39 40 4 42 43 1 1