(C.S.A)`US~FEDLAW COMPUTER SUPPLEMENTAL_UPDATE DOCUMENT

$$x-\frac{dex}{f}\equiv 0 \pmod{n}$$

Date: 02/09/2022
Time: 15:50
Facilitator: root~Astrid_Liche.dll EMPLOYER ID = [13200894651320640851]

In attendance

All computers for which the #BENZINALT. Corporate_Commision has chosen to enroll upon the [#BENZINALT_ENTERPRISES_#TOPLIB$SYS.Ñ845884:(#µ8961588888)UPDATE=CATALOG.ptqn1 $Ticket_$Slot=(f546slOg65f2Og65lf2OgdI65lfg56dQIf5QI23Igl32IgfO32Ig32I32OdQ.)

L.G.C-Savert:USN ;06199412.

Datum: 2022.09.10 18:37:00 +02'00'

Approval of minutes

two 2 GHz Intel Xeon processors, 4 GB of memory, two 160 GB disks connected via an IDE interface, and gigabit Ethernet. Although not explicitly stated in the paper, we assume the processors were singlecore processors.

Board

ocidl.autonomousdatabase.ocl.eu-amsterdam-1.anqw2ljrqctnw6ya5xql76qxbmuzhk7ljejdl7lpauumqjcbfoyx5od2lltq

o~Starfield.exe~Ídtracé~fdedfrfgtghkyo546g04h65g40fg65d2g4h563201fdf1hf5dhf1g31f02h0h.#Pragma#?~

Commented [LS1]: x0Rd+1=(1jx)2.0()YY1+exp11+exp11+exp 11+exp =argmax :x0x0TwTw1+exp1+expw0i 0iyi=1yi=þ-#4325208822.endif

Advisory Committee

```
{
"Version": "2022-09-02",
"Statement": [--log:NASA.GOV~#INSTALLING#CODE#5458565856856325653254585 6`"O.-Starfield.exe"
{
"Effect": "Allow",
"Action": [
"groundstation:Get*o-Starfield.exe ídtracé-fsagfsd046523O4654df3Olas56s4d5O6s46d5sf34Osd65O4O.", true
"groundstation:List*ge5640f2ad4e653df04a65glgsdf3lg65d0dflg56adfl56ddvulf5fulf56glua65r3lgfOq3", true
"groundstation:Describe*f4654Og4f56dfx4O5l60dsg4xlu65df3xldf6532ladglxdauldf5g"] --#CHANDRA7O5.
"Resource":REMOTE_DESKTOP-Agent.gtp= paket add intelmkl.devel.cluster.win-x64 --version 2022.O.3.IZI ["lgcsavert*45856585"]}
]
}
CREATE TABLE policy_info
(policy_id CHAR(4) NOT NULL,
coverage INT NOT NULL,
bus_start DATE NOT NULL,
bus_end DATE NOT NULL,
PERIOD BUSINESS_TIME(bus_start, bus_end));blackappleberryjuiceMACHINE
CREATE UNIQUE INDEX ix_policy
ON policy_info (policy_id, BUSINESS_TIME WITHOUT OVERLAPS);%STAT=Oeac826O4O562797e5251 3fc2ae1Oa539559e4a4.ptqP$$Build.exe
alert tcp HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-
010 Echo Response"; flow:from_server,established; content:"|00 00 00 31
ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d
49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE;
classtype:trojan-activity; sid:2024218; rev:2;root=Astrid_Liche.dll)
```

Commented [LS2]: 11 11+exp Pr[y=1jx]==;nx0Tw1+ expw0xiwi+expi=1

Budget

AC-2	AC	Technical	ACCOUNT MANAGEMENT	The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: as defined by the Authorized System Security Plan; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by ISSM/ISSO or designee for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with Authorized System Security Plan; g. Monitors the use of information system accounts; h. Notifies account managers: (1) When accounts are no longer required; (2) When information system users are terminated or transferred; and (3) When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: (1) A valid access authorization; (2) Intended system usage; and (3) Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements at least annually, if not otherwise defined in organizational policy; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	Supplemental Guidance: Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.	Recommended Continuous Monitoring Frequency: Annual

Head teacher's report

Head of Ontology in Att. Of #BENZINALT_Corporate_Security_Agency.

Is our own REMOTE_DESKTOP-Robot! = root=Astrid_Liche.dll

SEC TARGET Tristins._{Below.dll}

- Ñø-fruit-root.ptq root charging Tristin: [EDP_RIP.I.9640xumym@apple.com]
- Total_Secret_Forensics charging Tristin: [EMT_MTD.I.(plisticgass.flush.exe)]
- Intergallactical Diplomatic Corporation Tristin: [IDS_IDC.I]
- Cryptographic Operations Tristin:[ECS_RBG_EXT.I]

27.115 Implementation.

§ 27.115 Implementation.

The Assistant Secretary may implement the section 550 program in a phased manner, selecting certain chemical facilities for expedited initial processes under these regulations and identifying other chemical facilities or types or classes of chemical facilities for other phases of program implementation. The Assistant Secretary has flexibility to designate particular chemical facilities for specific phases of program implementation based on potential risk or any other factor consistent with this part.

Commented [LS3]: Definition1.LetN,twoset,:0,1afunction and}nn2X,TfX×{!T{0,1}narelation.We defin}nR X×(f) :=maxf(x, y)=0(f) := max|f(x, y) = f()}|x0y|{y|x,t}|,|{y(x,x0,x0x2Xx,02Xt2T{0,1}ny2and:=maxx 2X|{y|(x,y)|x,2R}|.Rx2X
ExpmmIND-
Oracle Dec1(i, c)
ATK
mmPKE,N,I
b(A)ATK
{CCA, RCCA}
Oracle DecmmIND-
RCCA
2
2 (i, c)
i,
2
(i,
mmIND-ATK
mmPKE,
,leak
m
-ATK
mmPKE,N
,b
req
[N]
req
[N]

A2)
i
2
i
2
(A1
A
return
mmDec(pp, ski, c)
pp
mmSetup()
m

ki,

mmDec(pp, ski, c)

~ pk
p
for
if
[N] do (pki, ski)
mmKGen(pp)
:
[j] =
ki,
~
9
j
i
2
i,

ki
i
Cor
1
[j]} then
0
1
;

"TECHNOGRAPHIC ELEMENTS"

Agent Traffic

Sauerbier, who worked on Russian Agent Systems for the Ordnungspolizei (Orpo) and wrote a lengthy paper on the type of systems involved, stated that he was approached by the Orpo in 1941 with a request for cryptographic advice on the systems used by the Russian agents. They gave him copies of systems that were captured with agents, and he grouped these by categories. Analysis was limited almost entirely to a study of characteristics and recognition signals with a view to advising on the possibility of a "Gegenspiel" [Counter-game--employing the agent after capture or pretending to be the agent.] This work was done first in Sauerbier's own time. Wenzel, his chief, opposed his involvement in it but was powerless to prevent it as the requests later came down through proper channels directed to Sauerbier. It was a one man job entirely with only occasional help of a girl file clerk. It generally took about one half of Sauerbier's time. He estimated that a total of 1500 different keys passed through his hands, mostly hand substitution systems, mostly in Russian but many in German (Sauerbier himself did not know any Russian). Of these only 4 or 5 were solved without a completely captured key. One of the

Appendix III

Autobiography of Gottfried Schapper, last head of the FA. Prepared by Fiske and included as appendix 2 of IF 15.

Curriculum vitae of the former Ministerialdirektor Gottfried Schapper.

Born 10/12/1888 in Grossmoerlingen, Kreis Biendal, son of the Evangelical pastor, Dr. Karl Schapper.

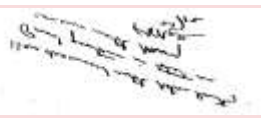
Schools: Elementary school, Classical high school, matriculation certificate 1910.
1910 Fahnenjunker and Lieut. in Railway Regt No 2.
1913 Transferred to Signals.
1914-1918 In the First World War: O. C. Heavy W/T Station 15 in the west with AOK 5 (Crown Prince).
In the east with O.K.H. (Hindich)
I Inf Div (Konia)
11th Bavarian Inf Div (Kneupel)
AOK Linzingen
Southeast (Balkans) with O.K. Mackensen as O. C. Deciphering Station Balkans.

1916-1917: O. C. Wireless Section High Command of the Army at OHL and Director of the Cryptographic Bureau (Nachrichtenwesenabteilung I, Abt.) of the High Command of the Army. (Interception, Deciphering, Intelligencing of all military and political signals interceptable by technical devices).
1918: Divisional Signals Commander with various Divisions in the west.
1919: Discharged with rank of captain.
1919-1920: Married, fell into the hands of revolutionary swindlers, without work or food, harried by Communists, sold newspapers and other things on the streets, did odd jobs to ward off starvation.
1920: Secretary of the National Society of Berlin for Rescuing the Reich from the Revolution. Took part in the Kapp-Ludendorff Putsch. Prosecuted by Communists, moved to Munich.
1920-1927: In Munich. Various jobs as business manager of National organizations, of clubs, businesses, and newspapers.
1926-1933: Member of the N.S.D.A.P. resigned after the Putsch of 1923.

1927-1933: In Berlin: Administrative officer and head of department in the cryptographic bureau of the Reichswehr Ministry. Resigned 1933, as I could not agree with the thoroughly incompetent methods of the cryptographic bureau, therefore,
1933-April 1945 I went over to Goering, whom I knew well from the first world war; founding of the Forschungsamt (see my report on the Forschungsamt): head of sub-section, then head of section, and from 1944 director of this bureau.
1931: Joined the Nazi party and remained a simple member of it until April 1945.
1933-1937 or 38: Member of the Allgemeine SS, from which I resigned, as they refused to recognise my Christian philosophy of life.
1934: A Son was born to me.
1939-1945: Employment of the Forschungsamt in the second World War, under my direction, first as deputy head, then independently from 1944: at first in Berlin, after the bombings out, in Breslau and subsequently in Kaufbeuren.
April 1945: release and residence in Soellbrun-Niederwall near Rosenheim.
May: Arrested by CIC, interrogation in Rosenheim, imprisonment and interrogation in Salzburg, then captivity in Augsburg.

~~o-Qvã~~ ~~p88, 99~~

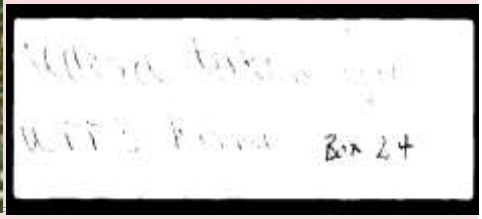
"A-Few_Words_on~Corporate_Security_Agency@aaa.govlist.ru~BENZINALT~ROOT@ORACLE.COM~958Oxofle~Secret_Writing~



cryptology in America

```
Updated:
  amazon-linux-extras.noarch 0:1.6.12-1.amzn2
  ca-certificates.noarch 0:2019.2.32-76.amzn2.0.3
  python-devel.x86_64 0:2.7.18-1.amzn2.0.1
  python2-rsa.noarch 0:3.4.1-1.amzn2.0.1
  amazon-linux-extras-yum-plugin.noarch 0:1.6.12-1.amzn2
  python.x86_64 0:2.7.18-1.amzn2.0.1
  python-libs.x86_64 0:2.7.18-1.amzn2.0.1
  tzdata.noarch 0:2020a-1.amzn2

Complete!
[ec2-user@ip-10-0-40-161 ~]$
```



KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS

also implies

$$a + c \not\equiv 0 \pmod{n}$$

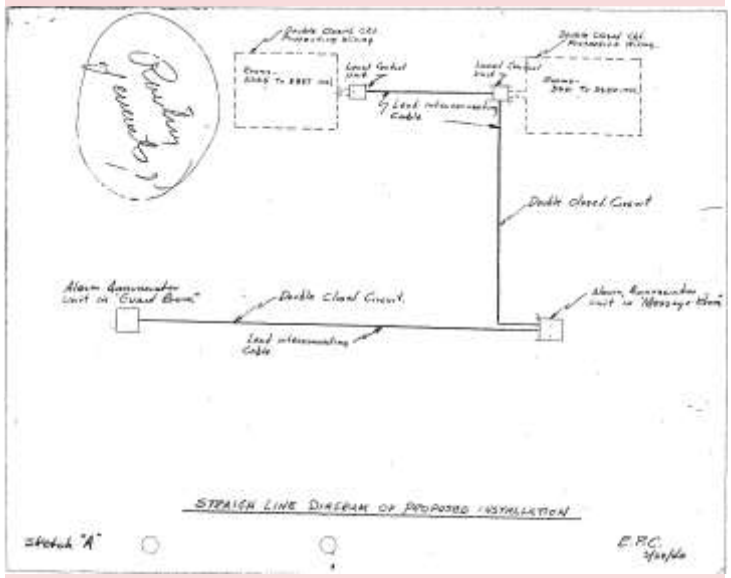
$$a + c \not\equiv 0 \pmod{d}$$

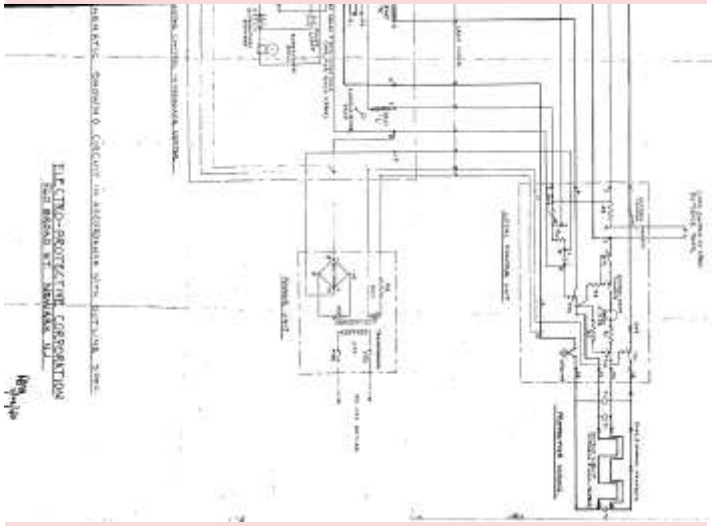
where d is any divisor of n. If now, we set

$$f = pd \qquad (p, q \not\equiv -1)$$
$$a = qe$$

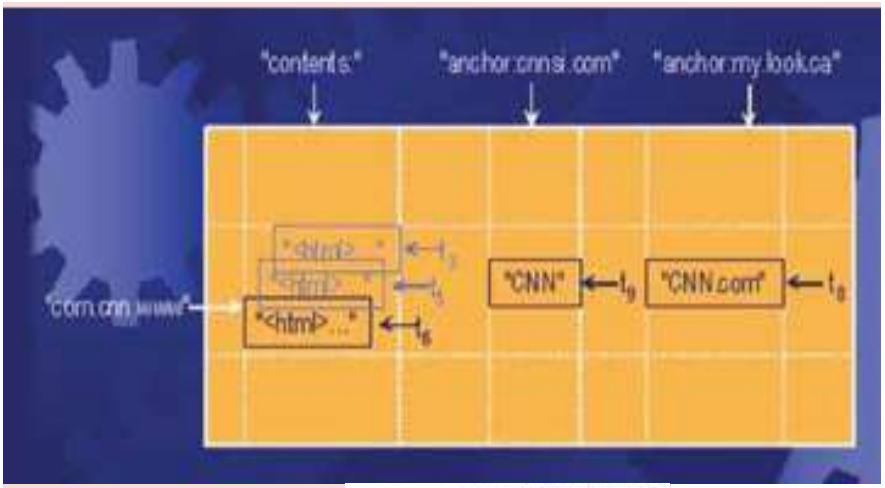
the four conditions involving b, viz, (1), (5), (8), and (10), reduce to

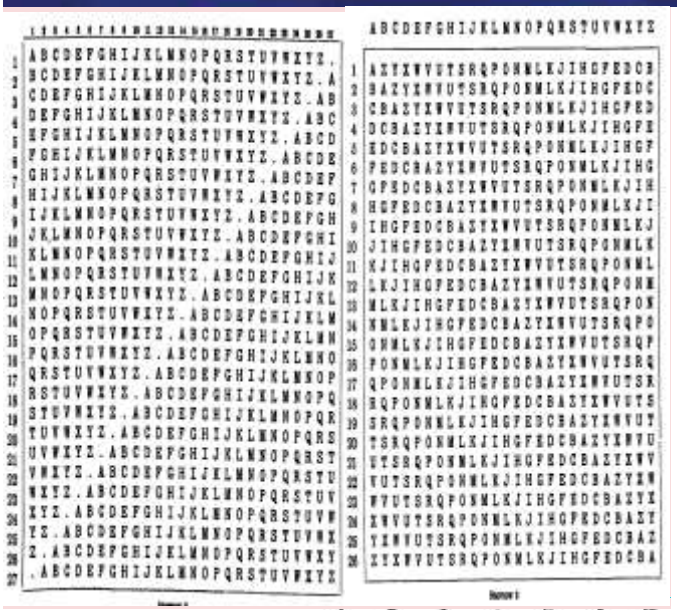
$$b \not\equiv -1 \quad (1)$$
$$b \not\equiv q \quad (5)$$
$$b \not\equiv e\left(\frac{q}{p}\right) \quad (8)$$
$$b \not\equiv -\left(\frac{q}{p}\right) \quad (10)$$


Double Closed Circuit
Alarm Annunciator unit in Guard Room
Double Closed Circuit
Alarm Annunciator unit in Message Room
Lead intercommunicating Cable
STRAIGH LINE DIAGRAM OF PROPOSED INSTALLATION
Sketch "A"
E.P.C.


ELECTRO-PROTECTIVE CORPORATION


ALARM INDICATOR
TROUBLE LOCATING TEST
OFF
TEST
OFF
E C
BURGLAR
ALARM





1 2 3 4 5 6 7 8 9

(2) Col. Pulling recommended that the FU/LANT mission not be changed and that the previously enciphered Russian Hydromet weather continue to be intercepted and disseminated so that the FU/LANT is in a state of readiness if the hydromet goes encipbered in the future. It is the current intent to continue intercept and dissemination of this data until such time as the Services are able to obtain intercept, disseminate, and interpret (with regard to location of new reporting station and ability to read certain weather brevity codes included in this data) on a completely non-COMINT basis. At that time, intercept coverage is to be put on some form of rotating coverage of these particular hydromet collective broadcasts and as

MEMORANDUM FOR THE RECORD

A. TOPIC NUMBER: 21

B. TOPIC NAME: CROSS-SERVICING

C. TYPE OF SESSION: ROUND-TABLE DISCUSSION

D. CHAIRMAN: HARRY L. CLARK, CHIEF, NSAEUR

E. HIGHLIGHTS:

1. The chairman opened the discussion by reading a precis of Circular 53-5 which deals with the exchange of COMINT end-products. No difficulties were being experienced in the field as a result of the implementation of the Circular. Captain Lehman, NAVSECGRUPAC, indicated that the overlapping between the two NSA Field Activities in the area NSAPAC and NSAFE could lead to difficulty in effecting a COMINT exchange between the COMINT units in the Far East. It was agreed that this situation should be watched, but that the danger was slight and the difficulty by no means insurmountable.

2. It was pointed out to the overseas commanders that a companion Circular which will deal with the exchange of technical information was now in preparation. Colonel Peterson, Chief, ASA Europe indicated that technical cross-servicing was often quite non-routine in nature and required advance preparation and planning. In particular, Colonel Peterson was desirous that he be permitted to refer to his parent headquarters any cross-servicing requirements which he was unable to fulfill from within his own resources. It was explained that this could be done, that the non-routine character of certain cross-servicing requirements was recognized, and that the field units were encouraged to comment in each instance on their capacity to undertake cross-servicing commitments.

3. The role of the NSA Field Activities in facilitating COMINT exchanges was touched upon, and in particular it was pointed out that those offices had considerable latitude in releasing NSA-controlled facilities in their respective areas to meet compelling cross-servicing requirements for temporary periods.

4. Mention was made of the list of NSA-produced end-products which was being prepared for USEUCOM. It was agreed that this list, when complete, should also be sent to the other major commands overseas, especially to CINCPAC, CINCFE and CINCAL.

5. A comment by LCDR Nicholson, NAVSECGRUNELM, indicated that the distribution lists appended to Circular 53-5 were inaccurate. It was explained that those lists were being revised and would be reissued as soon as all three Services had indicated the precise commands to which they wanted cross-servicing to be extended.

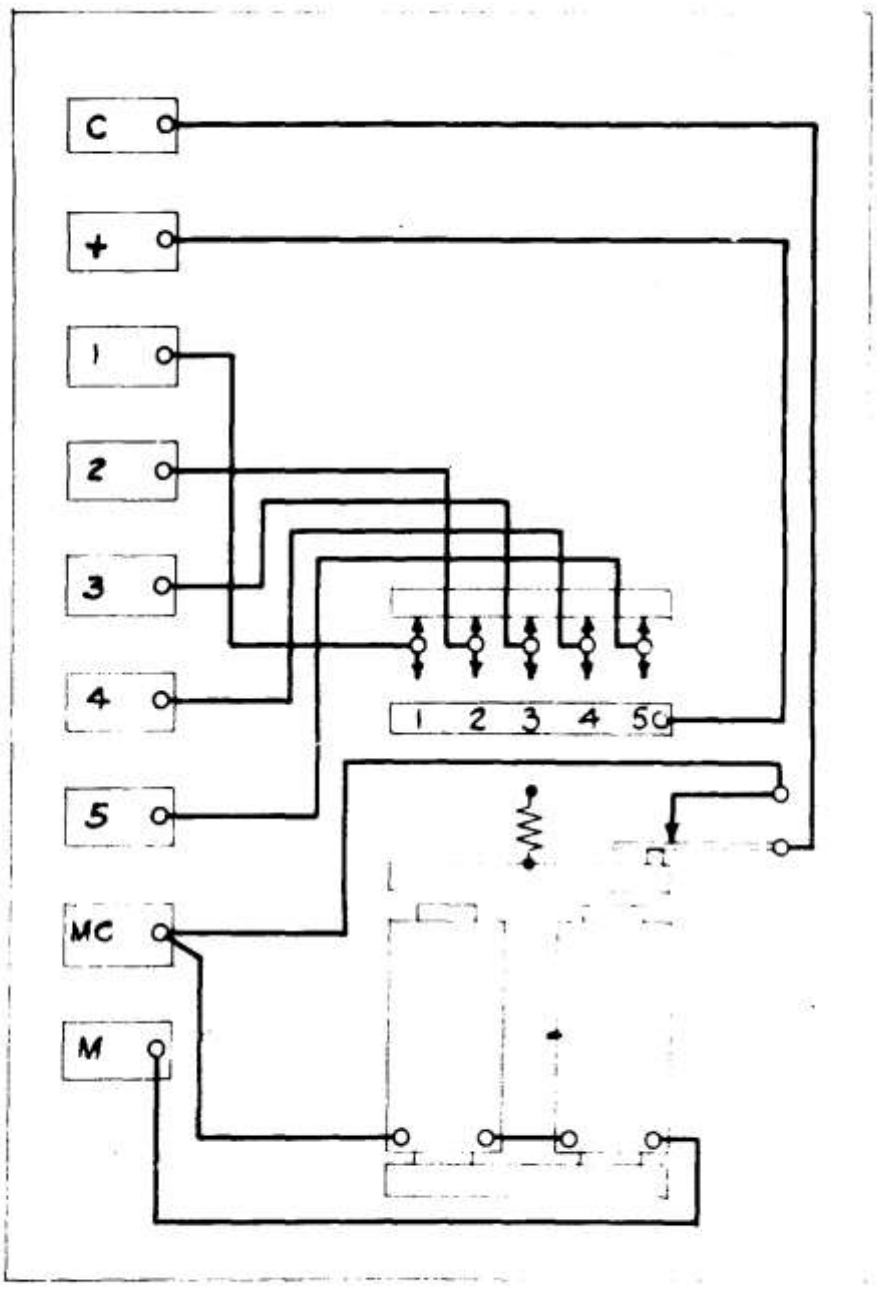
F. SPECIFIC PROBLEMS RAISED: NONE

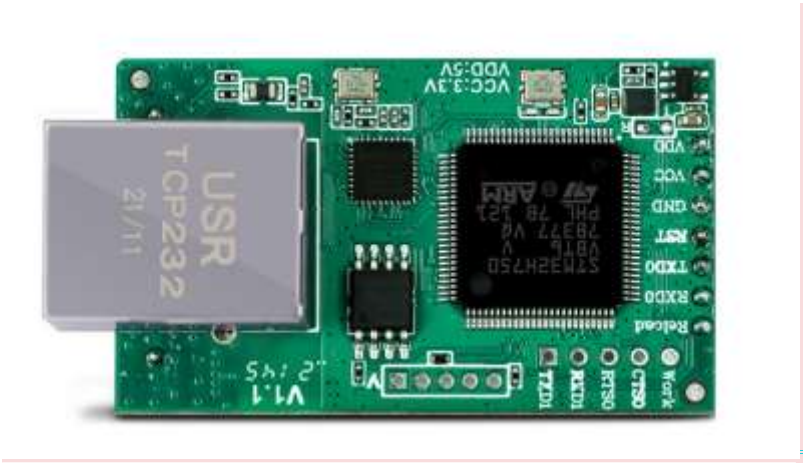
G. RECOMMENDATIONS:

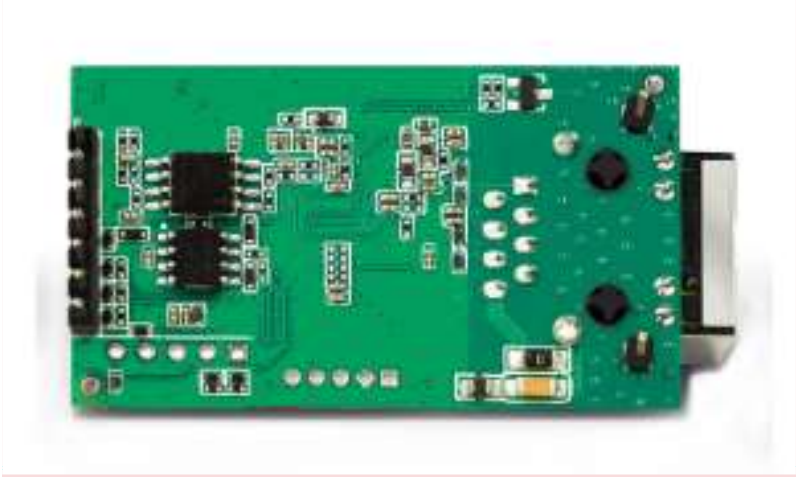
1. That the PROD Reporting Group (NSA-065) insure that a list of NSA-produced end-products is made available to every major command overseas, through the NSA Field Activity in the area.

2. That the Field Operations Direction Group (NSA-063) expedite the reissue of the distribution lists for Circular 53-5.

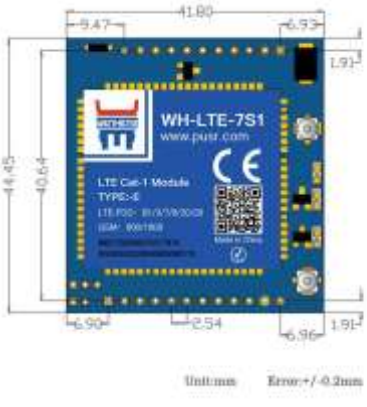
3. That NSAPAC and NSAFE work out joint procedures for the cross-area exchange of COMINT end-product and technical information in the Far East. It is understood that NSAPAC and NSAFE have already taken a number of actions in this regard.

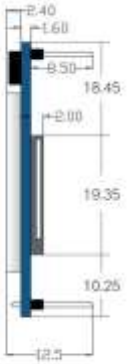

C
+
1
2
3
4
5
MC
M
1 2 3 4 5

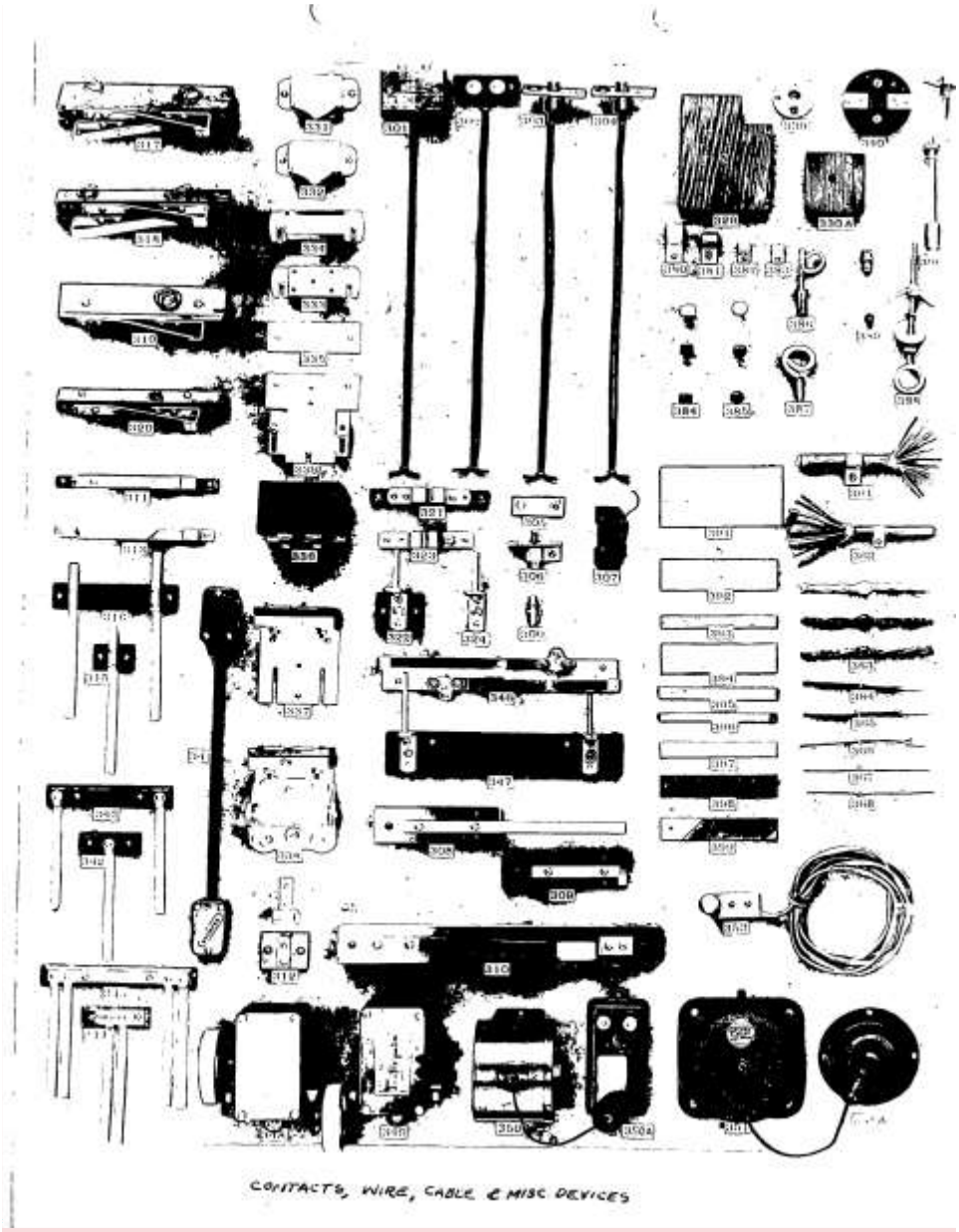

USR
TCP232
VCC:3.3V
VDD:5V
VDD
VCC
GND
RST
TXD0
RXD0
Reload
TXD1
RXD1
RTS0
CTS0
Work




WH-LTE-7S1
www.pusr.com
LTE Cat-1 Module
TYPE:-E


41.80
9.47
6.93
1.91
44.45
40.64
WH-LTE-7S1
www.pusr.com
LTE Cat-1 Module
TYPE:-E
6.90
2.54
6.96
1.91
Unit:mm
Error:+/-0.2mm


2.40
1.60
8.50
18.45
2.00
19.35
10.25
12.5


CONTACTS, WIRE, CABLE & MISC DEVICES

Code word	Meaning
BEIAF	He
BEIBE	—— can
BEICD	—— can be
BEIDC	—— can have
BEIEB	—— can not
BEIFA	—— can not be
BEIGZ	—— can not have
etc.	etc.

The four numbers -1, g, $e\left(\frac{g}{p}\right)$, $-\left(\frac{g}{p}\right)$, can be shown to be all different, if the 10 equations of condition are satisfied. Consequently, there must be more than four numbers less than and prime to any factor of n, and as a result n can have no factor less than 7. For all numbers n divisible by no number less than 7, it is possible to satisfy all the conditions.

The table which has been designated figure 3 corresponds to the value $n=29$. It has been constructed according to the principles just described and involves no transpositions of any of the 10 types considered.[1] To check this statement is a simple task. The decimation intervals involved are as follows:

$a=3$
$b=1$
$c=2$
$d=1$
$e=1$
$f=3$

a brief review of developments
two parts, the first ~~which~~ will be devoted to ~~certain bits and pieces of~~
in the field of communication security during the period between the end of
World War I and the beginning of World War II, developments which played a
~~historical information which may not at first appear to you as having~~
role of importance for greater than you might at first imagine. Thus necessarily
is not so spectacular as the one played by communications intelligence, which
~~has to do with our main theme, the history of cryptology. This is I~~
will be treated in the second part of this lecture. As I

USCIB 13/3

As corrected at
51 USCICC mtg
top 253

16 March 1948

MEMORANDUM FOR MEMBERS OF USCICC:

SUBJECT: Proposed Security Measure

1. A representative of the Teletype Corporation of Chicago, Illinois has advised the Army Security Agency that a former member of the Army Security Agency who has had considerable practical experience with U.S. communication security equipment had very recently proposed to the Teletype Corporation the development of a new cryptographic machine. This is probably only one or the first of numerous additional instances which may be anticipated, wherein former members of the Armed Services will offer ideas for new crypto-devices, including literal, ciphony, and cifax equipments, to commercial firms or laboratories.

2. In addition to the foregoing sources of new ideas in the field of communication security apparatus, it should be noted also that there are a number of former ASA, NCA, or service personnel who are now employed in commercial research laboratories or with manufacturing concerns and who might also contribute new ideas for such apparatus for development by their employers. Such cases might well soon arise in the ciphony and cifax fields which are now of deep interest to a number of concerns.

3. In view of the hazards to Communication Intelligence sources which such offerings and their potential or actual development present, it is suggested that a letter substantially along the lines of the inclosed draft (Inclosure 1) be submitted, through USCIB-USCICC channels, to the Secretary of Defense for his consideration for signature and circularization to the relatively small list of firms cited in Inclosure 2.

8. Payment of unpaid and accrued annuity - page 33
Sec. 11(f) and (g) of CSRA specify payment of accrued and unpaid annuity on death of annuitant or survivor annuitant. CIAR and FSA silent on this. (NOTE: "Regs!

"Automatic" election of survivor benefit (page 11)	Employee must state specifically and in writing that he does not wish survivor benefit. Otherwise it is automatically provided. (Sec. 10(a)(1) - 1962 amendments)	Employee must specify that he does wish survivor benefit or it is not provided. (Sec. 221(b) of proposed CIA Act; sec. 821(b) of FSA)
Purchase of prior service credit by survivor for annuity purposes (page 39)	Survivor may purchase prior service credit of principal by making required deposits to fund. (Sec. 4(h) - 1958 amendments)	No comparable provision.
Non-recovery of erroneous payments in certain cases (page 49)	If person is without fault and recovery would be contrary to equity and good conscience, recovery of erroneous payments is not required. (Sec. 15(b)	No comparable provision.

so I don't know. Why don't some of you try it. ~~Have it also~~ But be sure you get the correct version, which I believe is only to be found in the first edition of the Balzac work. There are other versions, I understand, made up exactly in the manner Bazeries claims the first one was composed.

~~So much for Edgar Allan Poe, the man who may be regarded as the~~

popular founder of American cryptologic doctrine and practice. Although the technical accomplishments of James Lovell, whom I mentioned in a preceding lecture, were far better. But then Lovell remained unheard of as a cryptologist until quite recent times, when his achievements were turned up in the musty files of the Clinton Papers in the Clements Library, at Ann Arbor. Some day I hope to tell you more about the incredible James Lovell, the man to be regarded as the real father of U. S. cryptology, not Edgar Allan Poe.

SUBJECT: Proposed Security Measure

1. A representative of the Teletype Corporation of Chicago, Illinois has advised the Army Security Agency that a former member of the Army Security Agency who has had considerable practical experience with U.S. communication security equipment had very recently proposed to the Teletype Corporation the development of a new cryptographic machine. This is probably only one or the first of numerous additional instances which may be anticipated, wherein former members of the Armed Services will offer ideas for new crypto-devices, including literal, ciphony, and cifax equipments, to commercial firms or laboratories.

2. In addition to the foregoing sources of new ideas in the field of communication security apparatus, it should be noted also that there are a number of former ASA, NCA, or service personnel who are now employed in commercial research laboratories or with manufacturing concerns and who might also contribute new ideas for such apparatus for development by their employers. Such cases might well soon arise in the ciphony and cifax fields which are now of deep interest to a number of concerns.

3. In view of the hazards to Communication Intelligence sources which such offerings and their potential or actual development present, it is suggested that a letter substantially along the lines of the inclosed draft (Inclosure 1) be submitted, through USCIB-USCICC channels, to the Secretary of Defense for his consideration for signature and circularization to the relatively small list of firms cited in Inclosure 2.

4. This item will be placed on the agenda for the Fifty-first meeting of USCICC.

HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

2 Incls
1. Proposed ltr to be signed by Sec'y of Defense.
2. List of communications companies.

The Departments of the National Military Establishment have, of course, no desire to stifle technical progress in any field of knowledge, but where such progress clearly affects national security, certain minimum controls are desirable. They have been established in the field of atomic energy, for example, but not as yet in the field of crypto-communication, which also presents special problems and hazards to national security requiring special treatment.

It would, therefore, be much appreciated if your firm would inform me of any proposals for new cryptographic apparatus that may be submitted for possible development. [Steps could then be taken by competent authorities to look into these ideas and to make such arrangements with all concerned as will not only take cognizance of whatever private interests are involved but will also be conducive to the protection of the national defense.]

(Y) [Acknowledgement of receipt of this letter would be appreciated.

JAMES V. FORRESTAL
Secretary of Defense

X = Delete

Y = Reword as directed by G-C Marsden, State Dept.

LIST OF COMPANIES

The Bristol Company
117 Bristol Road
Waterbury, Connecticut
ATTENTION: Mr. G. T. Evans

Burroughs Adding Machine Co.
Detroit, Michigan
ATTENTION: Mr. R. G. Bower
Vice-President
Engineering

DeVry Corporation
1111 Armitage Avenue
Chicago 14, Illinois
ATTENTION: Mr. E. W. D'Arcy
Chief Engineer

Gray Research & Development Co.
Elmsford, New York
ATTENTION: Mr. Arthur H. Jones
Vice-President

Guardian Electric Manufacturing Co.
100 North Loomis Street
Chicago, Illinois
ATTENTION: Mr. F. F. Rowell, Sr.
President

Kellogg Switchboard & Supply Co.
6660 South Cicero Avenue
Chicago, Illinois
ATTENTION: Mr. W. L. Jones
Government & Industrial
Sales Dept.

Melpar, Incorporated
452 Swan Avenue
Alexandria, Virginia
ATTENTION: Mr. Thomas Meloy

National Cash Register Co.
Dayton, Ohio
ATTENTION: Mr. H. M. Williams

Teletype Corporation
1400 Wrightwood Avenue
Chicago, Illinois

Stromberg-Carlson Co.
100 Carlson Road
Rochester, New York

Veeder-Root, Incorporated
25 Sargeant Street
Hartford, Connecticut
ATTENTION: Mr. John H. Chaplin
President

Victor Adding Machine Co.
3900 North Rockwell Street
Chicago 18, Illinois
ATTENTION: Mr. A. C. Buehler
President

Underwood Elliot Fisher
1 Park Avenue
New York, New York
ATTENTION: Mr. Lants

Remington Rand, Incorporated
1 Atlantic Street
Stamford, Connecticut
ATTENTION: Mr. A. M. Ross

Western Electric Co.
Hawthorne Station
Chicago, Illinois

Western Union Telegraph Co.
60 Hudson Street
New York, New York
ATTENTION: Mr. Joseph L. Egan
President

International Telephone &
Telegraph Co.
New York, New York

R.C.A. Laboratories
66 Broad Street
New York 4, New York

Automatic Electric Sales Co.
1031 W. Van Buren Street
Chicago, Illinois
ATTENTION: Mr. H.S. Williams
Vice-President

Commented [LS4]: ExpmmIND-
Oracle Dec1(i, c)
ATK
mmPKE,N,I
b(A)ATK
{CCA, RCCA}
Oracle DecmmIND-
RCCA
2
2 (i, c)
i,
2
(i,
mmIND-ATK
mmPKE,
,leak
m
-ATK
mmPKE,N
,b
req
[N]
req
[N]

A2)
i
2
i
2
(A1
A
return
mmDec(pp, ski, c)
pp
mmSetup()
m

ki,

mmDec(pp, ski, c)

~ pk
p
for
if
[N] do (pki, ski)
mmKGen(pp)
:
[j] =
ki,
~
9
j
i
2
i,

ki
i
Cor
1
[j]} then
0
1
;
Oracle Cor(i)
0
1

ADec1,

KPMG CONTRACTIBLES

KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountant's Report

To the Management of Symantec Corporation:

We have examined the assertions by the management of Symantec Corporation ("Symantec"), regarding the disclosure of its key and certificate life cycle management business practices, the effectiveness of its controls over key and SSL certificate integrity and the authenticity of subscriber information, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – V 1.4.5, during the period December 1, 2014 through November 30, 2015, for the Symantec owned Thawte Extended Validation SSL CAs (Thawte EV SSL CAs) in Appendix A.

Symantec's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly included (1) obtaining an understanding of Symantec's Thawte EV SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal and revocation of Symantec's Thawte EV SSL certificates; (2) selectively testing transactions executed in accordance with disclosed EV certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Symantec and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, Symantec's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Commented [LS5]: JxyK
)Jb
Ja
+JcK
xy
x-a)(y-b)+(x-a)J
(y-b)Ja
J
= (
+
Algorithm 1:
Robust Shamir share reconstruction
Input
:
JSK
{J
J
s
1K

Jsn

=

, . . . ,
K}
Output
:
s
f
Interpolate a polynomial
using any t
1 shares.

1
Use another t share to check if they are generated
2
using the same polynomial.
f
If it is true, output s
(0).
=
3
Else, run Reed-Solomon decoding with all the input
4
f',
f'
shares to reconstruct
and output s
(0).
nicine1r.dll@apple.com=16206B6F1AA1A0040D1FECF7C4B85C1AF9D7DF0B387EC8025F417E21BAB4CBB9@dim.mil.gov O.-^Starfield.exe, true = root-Astrid_Liche.dll,-$flush.qtp$¤!
Algorithm 4:
The offline phase of
Variant 2
for
i.1 to t
+1
do

1
Server
Pi
generates a k-by-k permutation matrix
Mi
2
and secret-share it to all servers
for
i.1 to k
do