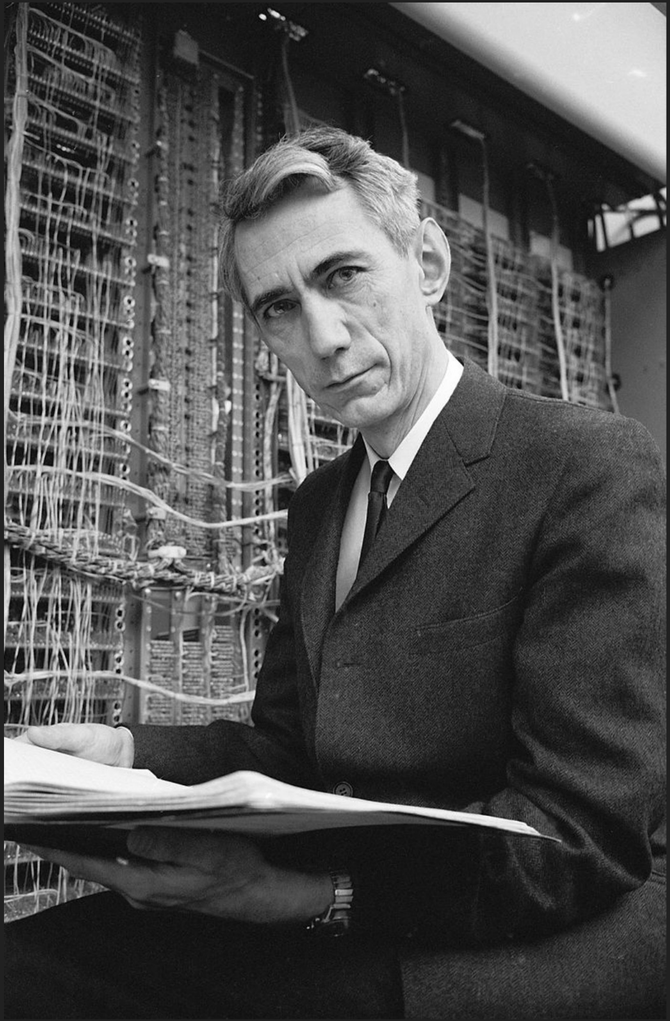
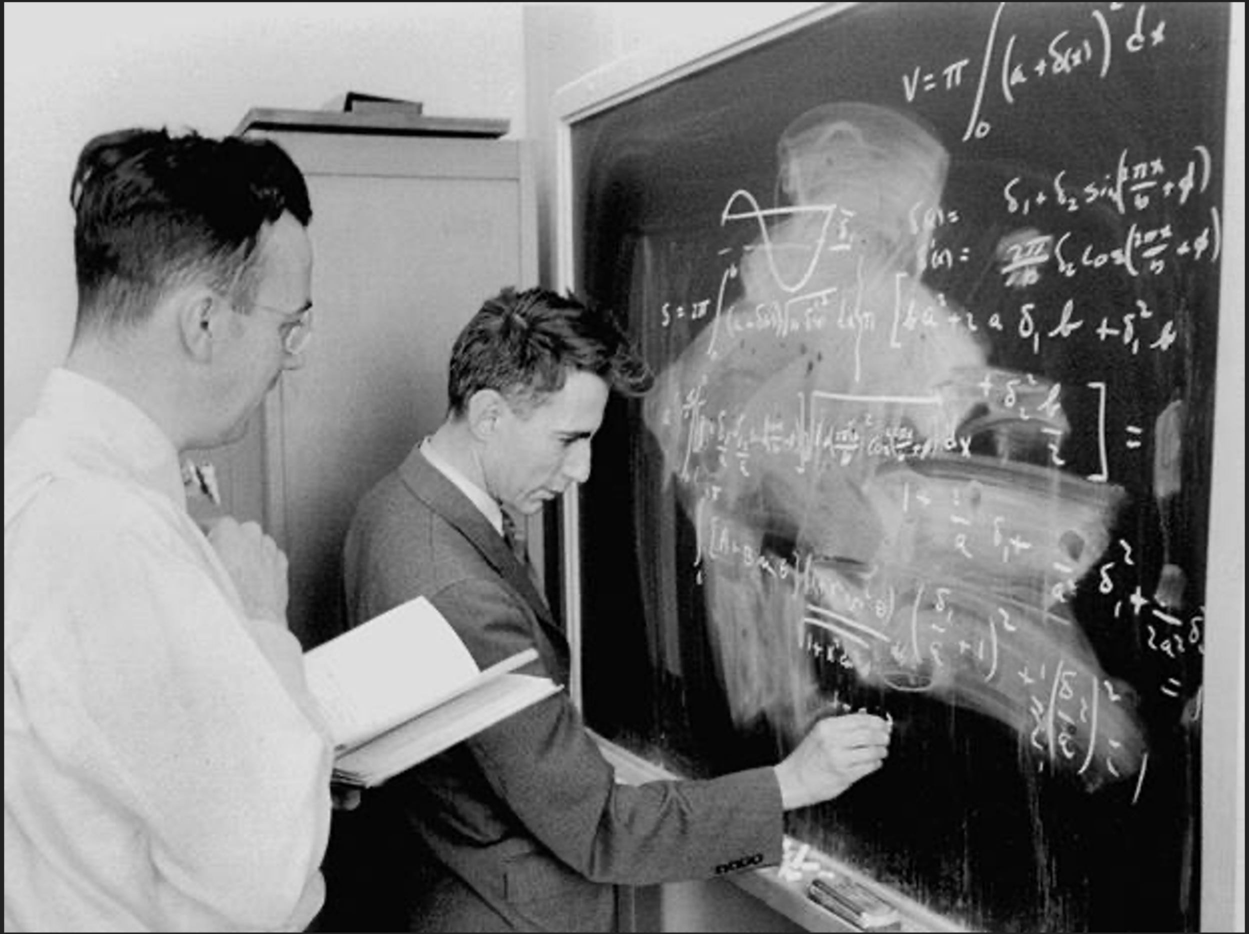
Gathering Randomness for the Vernam System

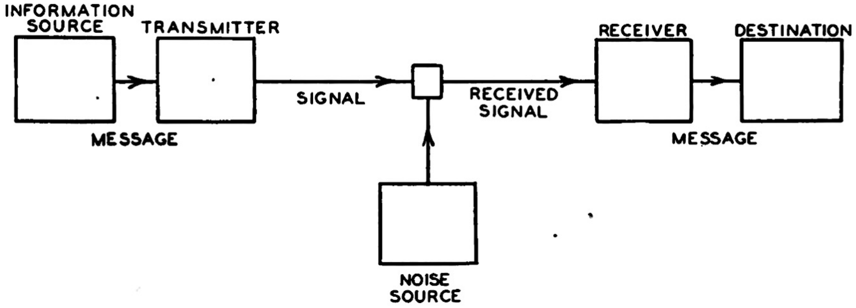
The Cryptographic Use of Noise at Bell Labs

Charles Berret
Columbia University

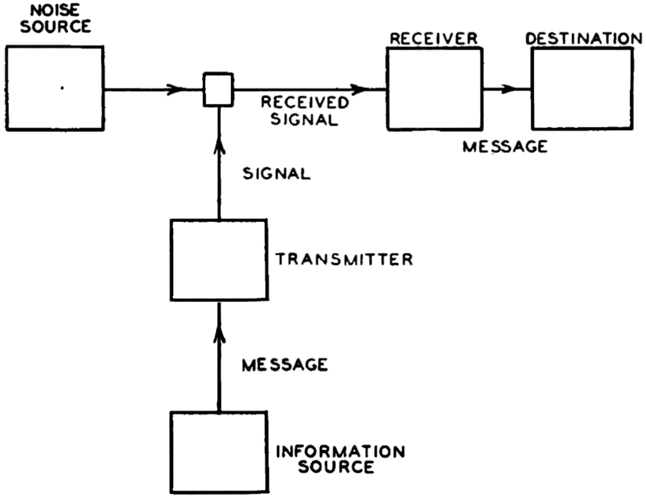
SHOT Annual Meeting
October 27, 2017



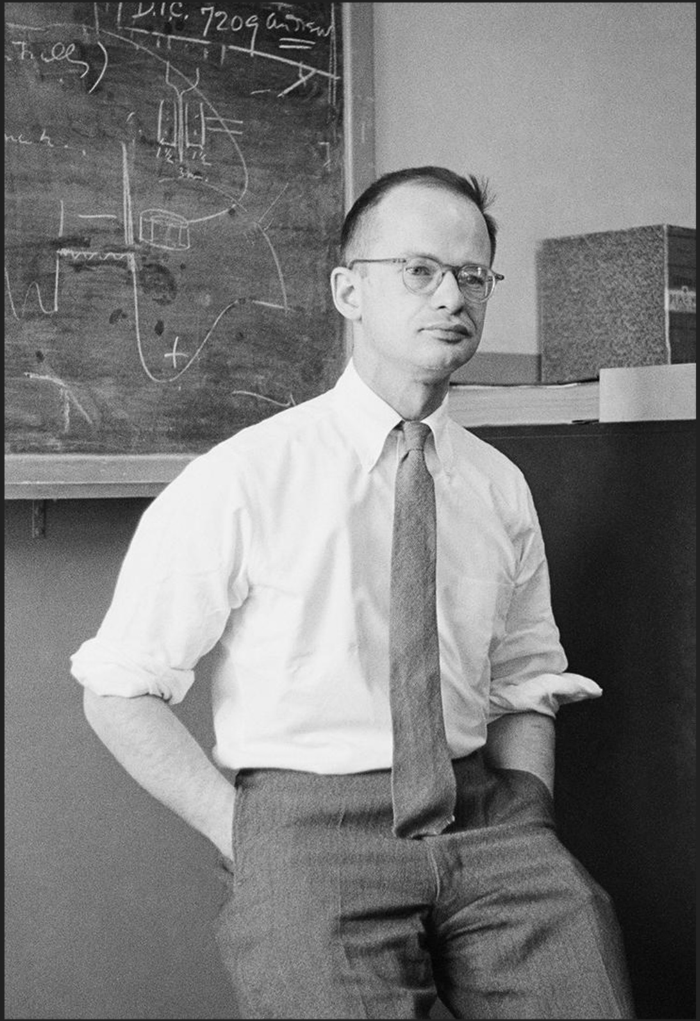




INFORMATION SOURCE
TRANSMITTER
RECEIVER
DESTINATION
SIGNAL
RECEIVED SIGNAL
MESSAGE
MESSAGE
NOISE SOURCE



NOISE SOURCE
RECEIVER
DESTINATION
RECEIVED SIGNAL
MESSAGE
SIGNAL
TRANSMITTER
MESSAGE
INFORMATION SOURCE



The Bell System Technical Journal

Vol. XXVII *July, 1948* *No. 3*

A Mathematical Theory of Communication

By C. E. SHANNON

Introduction

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

1. It is practically more useful. Parameters of engineering importance

[1] Nyquist, H., "Certain Factors Affecting Telegraph Speed," *Bell System Technical Journal*, April 1924, p. 324; "Certain Topics in Telegraph Transmission Theory," *A. I. E. E. Trans.*, v. 47, April 1928, p. 617.
[2] Hartley, R. V. L., "Transmission of Information," *Bell System Technical Journal*, July 1928, p. 535.

Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. Introduction and Summary

THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment systems are primarily a psychological problem, and privacy systems a technological one.

Secondly, the treatment is limited to the case of discrete information, where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.

The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to

* The material in this paper appeared originally in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1945, which has now been declassified.
[1] Shannon, C. E., "A Mathematical Theory of Communication," *Bell System Technical Journal*, July 1948, p. 379; Oct. 1948, p. 623.
[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

The Bell System Technical Journal

Vol. XXVII July, 1948 No. 3

A Mathematical Theory of Communication

By C. E. SHANNON

Introduction

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

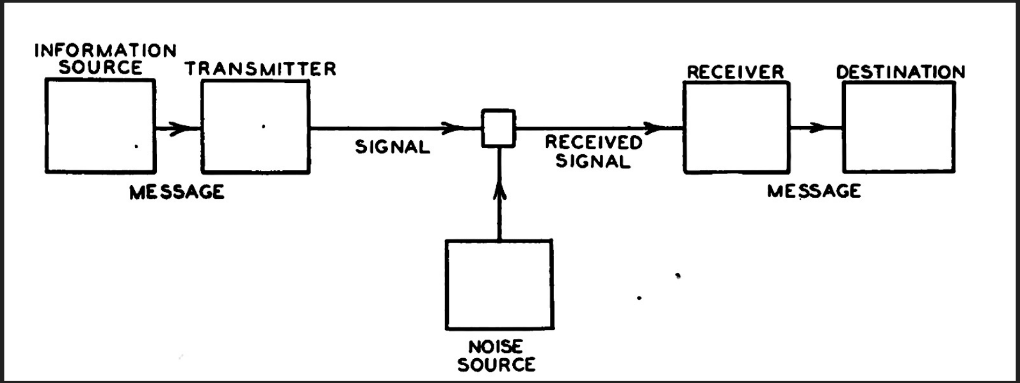
If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

1. It is practically more useful. Parameters of engineering importance

[1] Nyquist, H., "Certain Factors Affecting Telegraph Speed," *Bell System Technical Journal*, April 1924, p. 324; "Certain Topics in Telegraph Transmission Theory," *A. I. E. E. Trans.*, v. 47, April 1928, p. 617.

[2] Hartley, R. V. L., "Transmission of Information," *Bell System Technical Journal*, July 1928, p. 535.



Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. Introduction and Summary

THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment systems are primarily a psychological problem, and privacy systems a technological one.

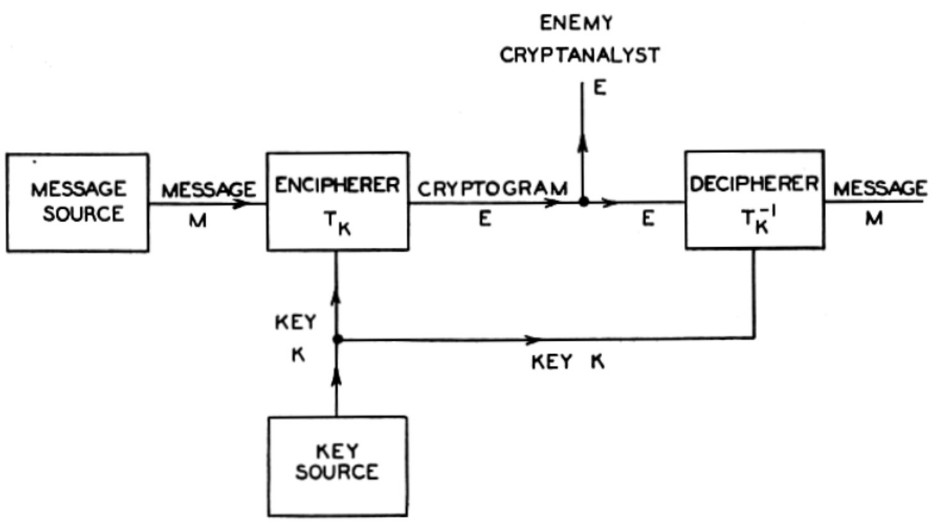
Secondly, the treatment is limited to the case of discrete information, where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.

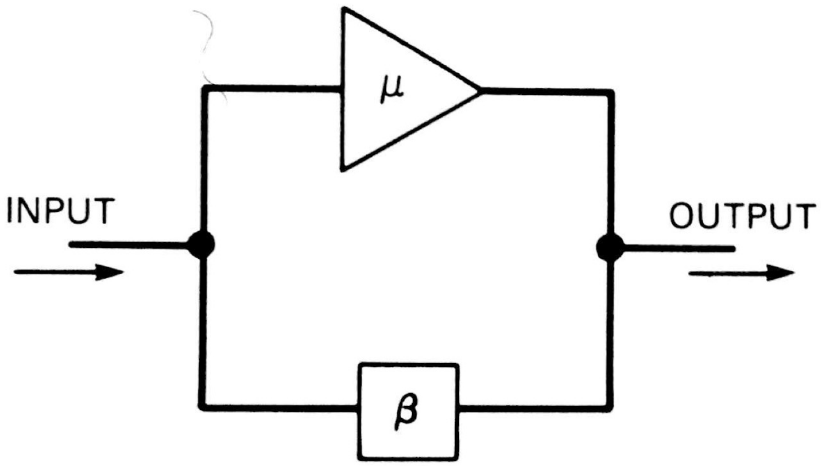
The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to

* The material in this paper appeared originally in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1945, which has now been declassified.

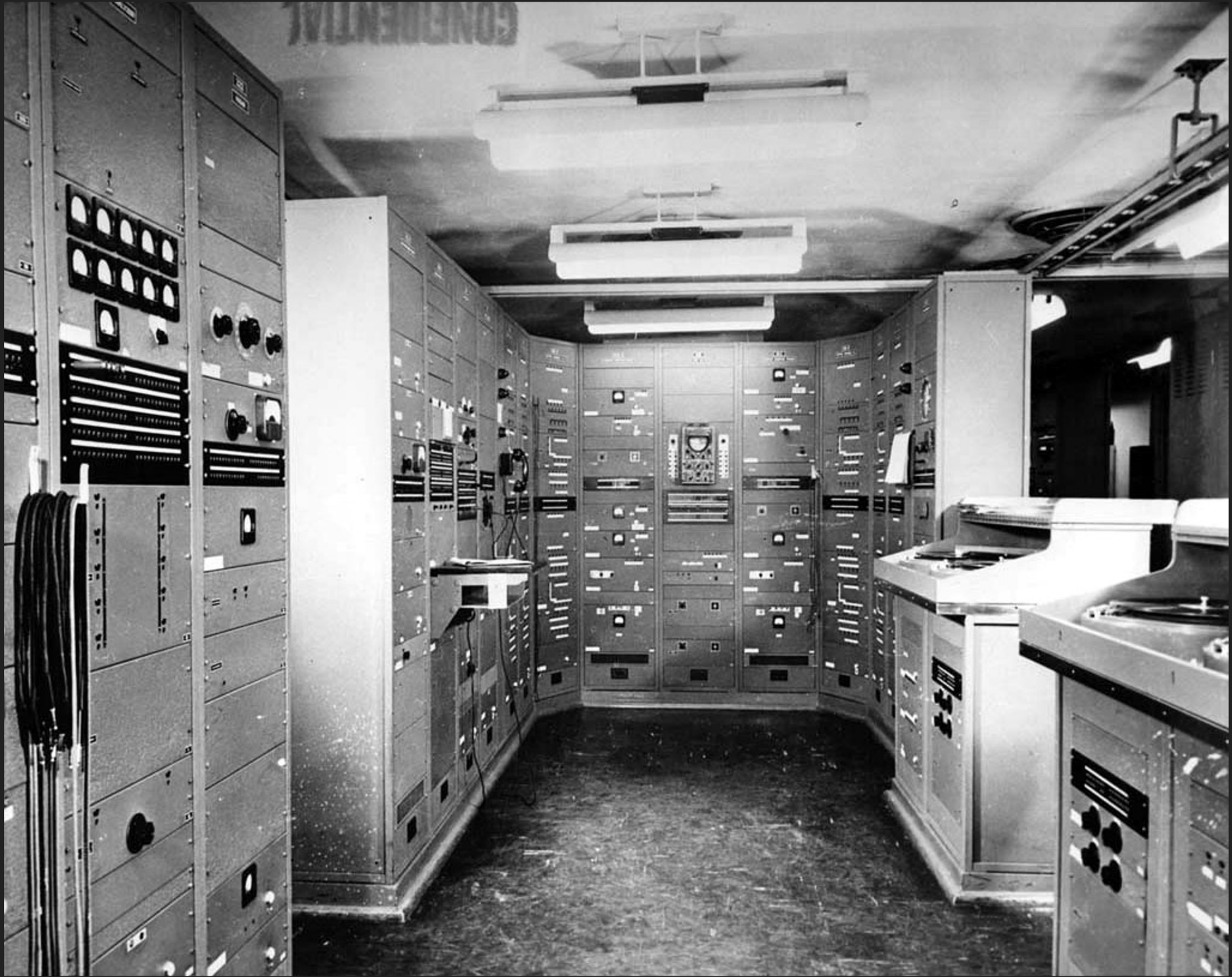
[1] Shannon, C. E., "A Mathematical Theory of Communication," *Bell System Technical Journal*, July 1948, p. 379; Oct. 1948, p. 623.

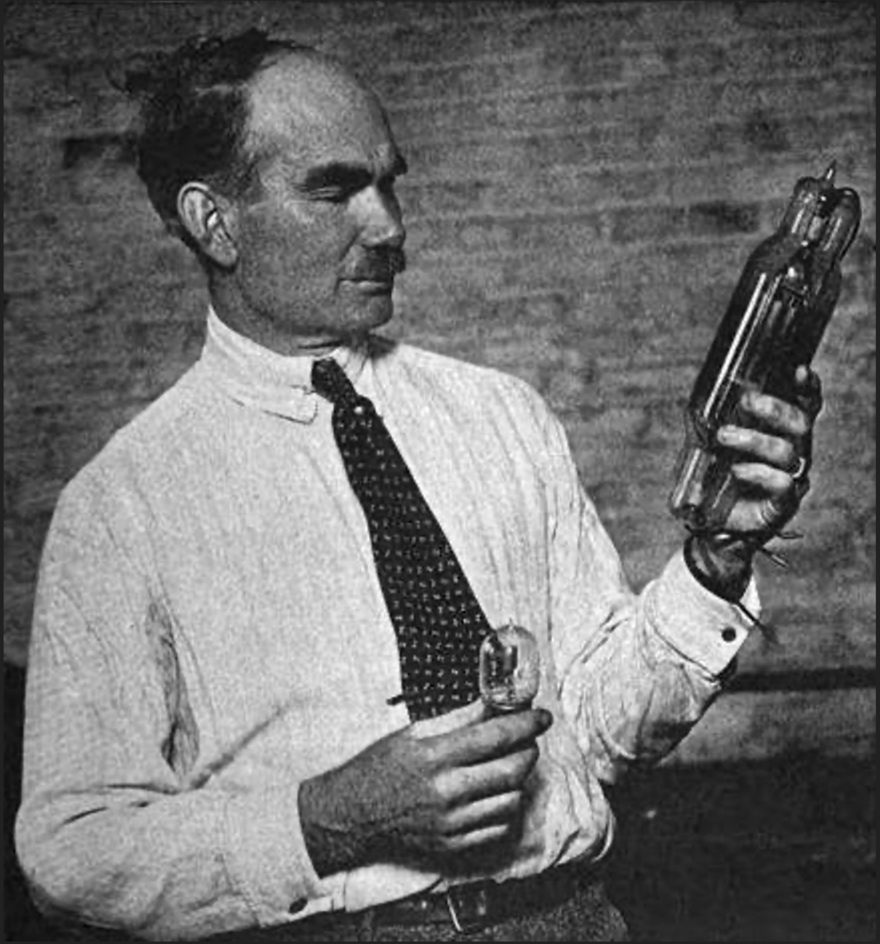
[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

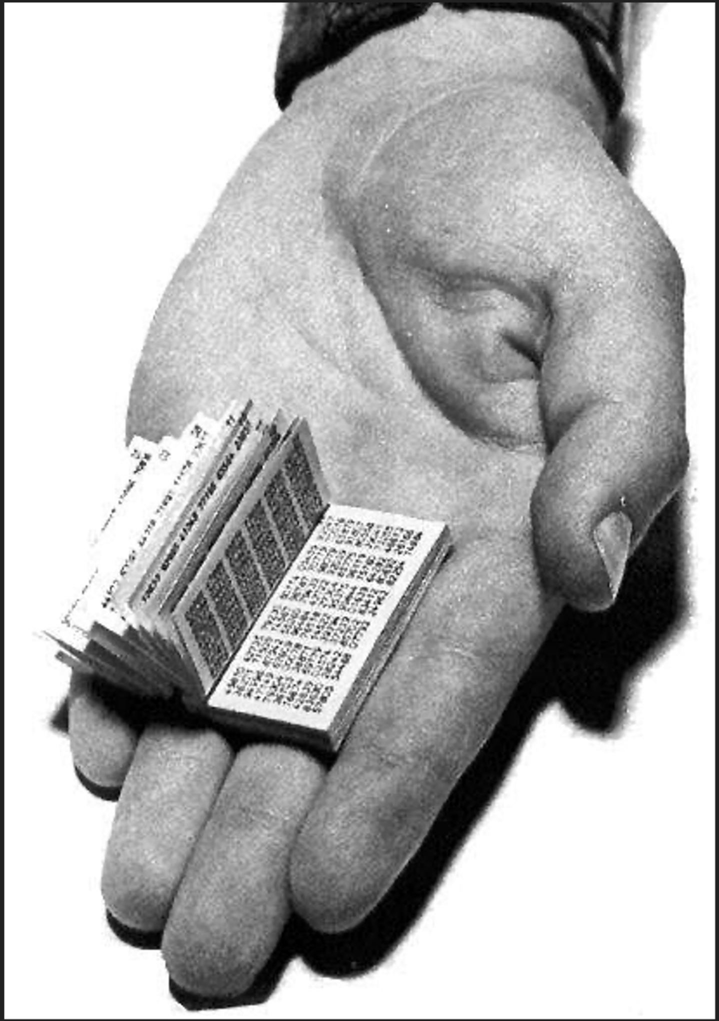


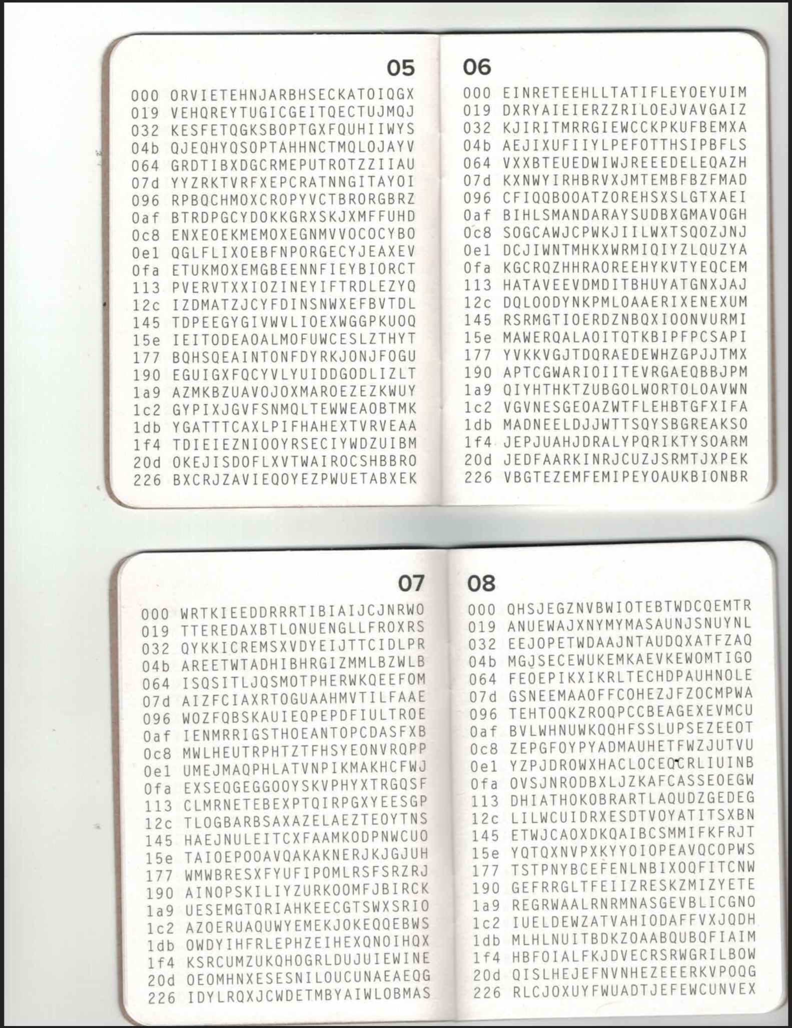


$$\frac{\text{OUTPUT}}{\text{INPUT}} = A_F = \frac{\mu}{1-\mu\beta} = \frac{1}{-\beta}\left[1 - \frac{1}{1-\mu\beta}\right]$$







05

000	ORVIETEHNJARBHSECKATOIQGX
019	VEHQREYTUGICGEITQECTUJMQJ
032	KESFETQGKSBOPTGXFQUHIIWYS
04b	QJEQHYQSOPTAHHNCTMQLOJAYV
064	GRDTIBXDGCRMEPUTROTZZIIAU
07d	YYZRKTVRFXEPCRATNNGITAYOI
096	RPBQCHMOXCROPYVCTBRORGBRZ
0af	BTRDPGCYDOKKGRXSKJXMFFUHD
0c8	ENXEOEKMEMOXEGNMVVOCOCYBO
0e1	QGLFLIXOEBFNPORGECYJEAXEV
0fa	ETUKMOXEMGBEENNFIEYBIORCT
113	PVERVTXXIOZINEYIFTRDLEZYQ
12c	IZDMATZJCYFDINSNWXEFBVTDL
145	TDPEEGYGIVWVLIOEXWGGPKUOQ
15e	IEITODEAOALMOFUWCESLZTHYT
177	BQHSQEAINTONFDYRKJONJFOGU
190	EGUIGXFQCYVLYUIDDGODLIZLT
1a9	AZMKBZUAVOJOXMAROEZEZKWUY
1c2	GYPIXJGVFSNMQLTEWWEAOBTMK
1db	YGATTTCAXLPIFHAHEXTVRVEAA
1f4	TDIEIEZNIOOYRSECIYWDZUIBM
20d	OKEJISDOFLXVTWAIROCSHBBRO
226	BXCRJZAVIEQOYEZPWUETABXEK

06

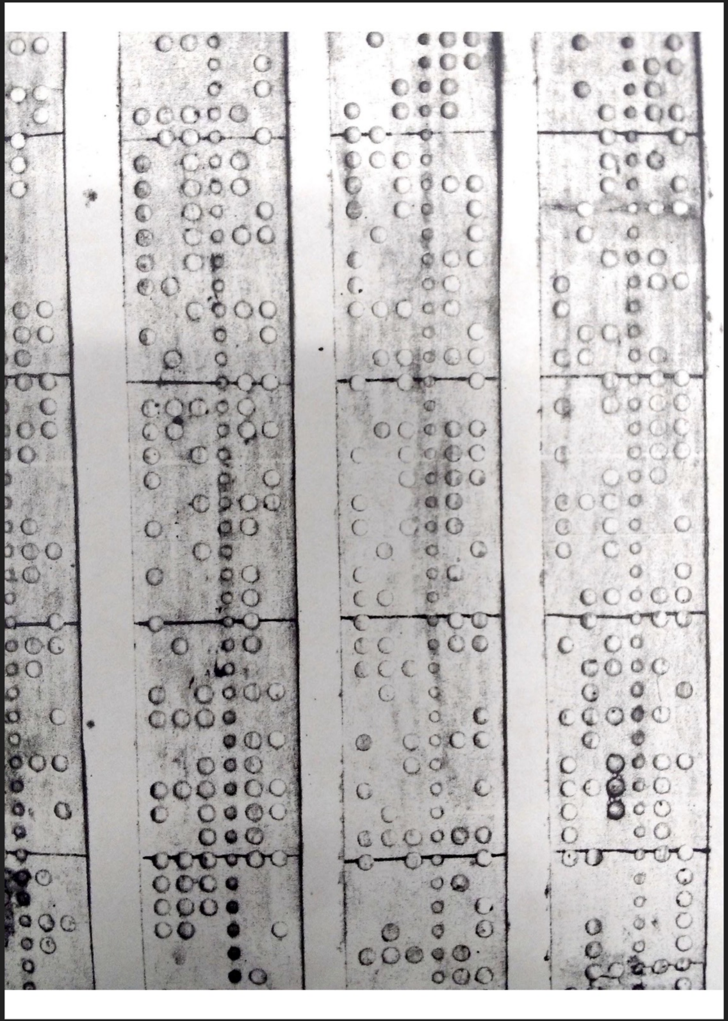
000	EINRETEEHLLTATIFLEYOEYUIM
019	DXRYAIEIERZZRILOEJVAVGAIZ
032	KJIRITMRRGIEWCCKPKUFBEMXA
04b	AEJIXUFIIYLPEFOTTHSIPBFLS
064	VXXBTEUEDWIWJREEEDELEQAZH
07d	KXNWYIRHBRVXJMTEMBFBZFMAD
096	CFIQQBOOATZOREHSXSLGTXAEI
0af	BIHLSMANDARAYSUDBXGMAVOGH
0c8	SOGCAWJCPWKJIILWXTSQOZJNJ
0e1	DCJIWNTMHKXWRMIQIYZLQUZYA
0fa	KGCRQZHHRAOREEHYKVTYEQCEM
113	HATAVEEVDMDITBHUYATGNXJAJ
12c	DQLOODYNKPMLOAAERIXENEXUM
145	RSRMGTIOERDZNBQXIOONVURMI
15e	MAWERQALAOITQTKBIPFPCSAPI
177	YVKKVGJTDQRAEDEWHZGPJJTMX
190	APTCGWARIOIITEVRGAEQBBJPM
1a9	QIYHTHKTZUBGOLWORTOLOAVWN
1c2	VGVNESGEOAZWTFLEHBTGFXIFA
1db	MADNEELDJJWTTSQYSBGREAKSO
1f4	JEPJUAHJDRALYPQRIKTYSOARM
20d	JEDFAARKINRJCUZJSRMTJXPEK
226	VBGTEZEMFEMIPEYOAUKBIONBR

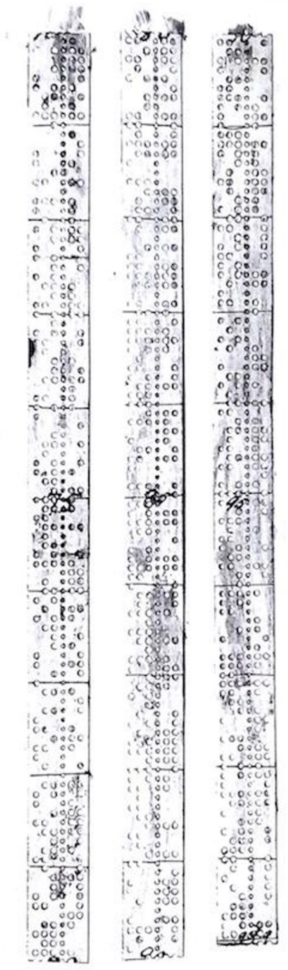
07

000	WRTKIEEDDRRRTIBIAIJCJNRWO
019	TTEREDAXBTLONUENGLLFROXRS
032	QYKKICREMSXVDYEIJTTCIDLPR
04b	AREETWTADHIBHRGIZMMLBZWLB
064	ISQSITLJQSMOTPHERWKQEEFOM
07d	AIZFCIAXRTOGUAAHMVTILFAAE
096	WOZFQBSKAUIEQPEPDFIULTROE
0af	IENMRRIGSTHOEANTOPCDASFXB
0c8	MWLHEUTRPHTZTFHSYEONVRQPP
0e1	UMEJMAQPHLATVNPIKMAKHCFWJ
0fa	EXSEQGEGGOOYSKVPHYXTRGQSF
113	CLMRNETEBEXPTQIRPGXYEESGP
12c	TLOGBARBSAXAZELAEZTEOYTNS
145	HAEJNULEITCXFAAMKODPNWCUO
15e	TAIOEPOOAVQAKAKNERJKJGJUH
177	WMWBRESXFYUFIPOMLRSFSRZRJ
190	AINOPSKILIYZURKOOMFJBIRCK
1a9	UESEMGTQRIAHKEECGTSWXSRIO
1c2	AZOERUAQUWYEMEKJOKEQQEBWS
1db	OWDYIHFRLEPHZEIHEXQNOIHQX
1f4	KSRCUMZUKQHOGRLDUJUIEWINE
20d	OEOMHNXESESNILOUCUNAEAEQG
226	IDYLRQXJCWDETMBYAIWLOBMAS

08

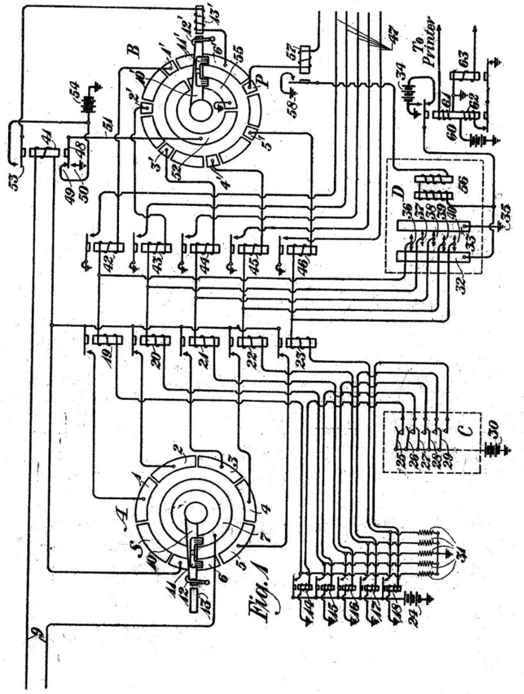
000	QHSJEGZNVBWIOTEBTWDCQEMTR
019	ANUEWAJXNYMYMASAUNJSNUYNL
032	EEJOPETWDAAJNTAUDQXATFZAQ
04b	MGJSECEWUKEMKAEVKEWOMTIGO
064	FEOEPIKXIKRLTECHDPAUHNOLE
07d	GSNEEMAAOFFCOHEZJFZOCMPWA
096	TEHTOQKZROQPCCBEAGEXEVMCU
0af	BVLWHNUWKQQHFSSLUPSEZEEOT
0c8	ZEPGFOYPYADMAUHETFWZJUTVU
0e1	YZPJDROWXHACLOCEQCRLIUINB
0fa	OVSJNRODBXLJZKAFCASSEOEGW
113	DHIATHOKOBRARTLAQUDZGEDEG
12c	LILWCUIDRXESDTVOYATITSXBN
145	ETWJCAOXDKQAIBCSMMIFKFRJT
15e	YQTQXNVPXKYYOIOPEAVQCOPWS
177	TSTPNYBCEFENLNBIXOQFITCNW
190	GEFRRGLTFEIIZRESKZMIZYETE
1a9	REGRWAALRNRMNASGEVBLICGNO
1c2	IUELDEWZATVAHIODAFFVXJQDH
1db	MLHLNUITBDKZOAABQUBQFIAIM
1f4	HBFOIALFKJDVECRSRWGRILBOW
20d	QISLHEJEFNVNHEZEEERKVPOQG
226	RLCJOXUYFWUADTJEFEWCUNVEX





209976
(2) 1

Secret Signaling System



Witnesses:

Certified to be the drawing referred to in the specification hereunto annexed.

NEW YORK. N.Y. U.S.A. DEC. 26 1919

INVENTOR.

G. S. Vernam

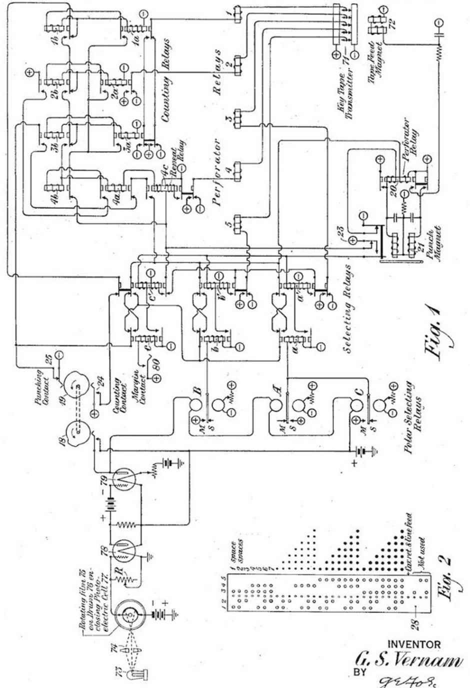
BY

ATTORNEY

Jan. 11, 1927. G. S. VERNAM 1,613,686

METHOD OF AND APPARATUS FOR SECRET ELECTRICAL TRANSMISSION OF PICTURES

Filed Dec. 5, 1924 2 Sheets-Sheet 1



INVENTOR

G. S. Vernam

BY

ATTORNEY

16850	20799	66620	68842	98194	66012	15684	51340	11255	00543	84815
16851	26475	77439	87749	28202	34961	77840	70008	43213	59116	10886
16852	66508	08863	98316	04572	98170	47008	90279	13986	88866	20250
16853	94534	79709	74264	86785	53209	75201	01423	25233	42178	82288
16854	27762	23951	92472	91602	81646	35621	34790	65655	18754	85297
16855	60298	00276	54600	94187	84908	92495	13362	21039	11824	98043
16856	97491	85012	82791	76682	29934	85360	36959	33683	17340	62742
16857	43940	34283	72358	66061	89486	37188	34089	21741	41559	62563
16858	45703	28014	98900	93228	15800	27375	17749	17687	48484	28963
16859	42574	96720	51400	97938	19221	32723	56132	43989	71962	88840
16860	39528	37612	81703	41333	56418	09349	85888	62179	19883	67992
16861	43395	48721	06939	00691	21000	11983	81743	54203	22673	62209
16862	11545	71679	15130	97968	35897	02802	50715	84710	01287	30756
16863	08369	62072	66992	65072	82543	08639	26553	72468	99724	97841
16864	24287	78099	94170	08751	78592	15297	22480	00619	19312	44214
16865	35389	21449	90068	67376	85902	18674	97864	31149	05179	63133
16866	66050	35878	19237	51696	03959	81319	66561	52550	39850	37731
16867	34215	27992	11989	43180	89551	33093	50506	18578	04991	89827
16868	81548	50795	19793	38557	95544	51205	45981	68698	37183	36457
16869	10798	35694	30060	87157	27128	49985	22982	36591	55770	68401
16870	20088	74967	60411	88025	73065	54993	37431	68500	00914	84510
16871	70795	81112	85906	22506	80200	41880	53183	18039	89235	02366
16872	30325	54766	93220	74778	69394	29880	38249	13143	56487	53469
16873	42893	81476	87682	12972	32490	71884	17051	15930	33106	49357
16874	18331	97115	84538	11061	73328	33583	50366	33222	07826	05218
16875	96540	00284	84227	84858	20423	93130	76393	85686	40929	04637
16876	38079	73233	91250	67075	01512	80197	02618	28569	50508	24060
16877	42366	17266	73202	20623	00803	84046	67598	66279	05642	25670
16878	18414	12694	62295	32343	36392	52451	88639	17257	38658	15322
16879	55286	30468	81212	38172	63105	29247	93288	33588	54256	93563
16880	30865	02157	82487	54593	80317	25137	47899	77649	28912	58164
16881	22495	72694	76620	66182	93724	66972	08908	57083	38703	40720
16882	87433	01700	20949	08219	10502	51633	69424	15874	86202	75889
16883	52903	02219	44376	07662	34539	65176	10558	26676	68966	27637
16884	59532	59191	66832	33034	39950	15435	30083	28580	27588	19066
16885	70350	28784	88290	55343	87238	55371	87310	52811	18779	21577
16886	88726	92056	97259	47453	20966	24962	79787	60704	55141	85543
16887	20507	29039	17302	77828	27938	04909	54396	33416	65721	05963
16888	01104	98156	33915	73433	96523	85888	75847	55351	57429	61939
16889	82039	37543	54979	36278	18345	20663	68679	80455	66905	61129
16890	05435	10525	13303	53439	57066	46325	61272	01028	27506	04668
16891	58884	47108	85374	75305	16104	35321	69694	86702	17280	27130
16892	08190	78070	91129	98765	10899	43799	93406	05313	06001	35715
16893	02300	91024	48844	98034	38473	85359	40334	63953	03621	67019
16894	55071	03428	52171	02310	96305	15792	07644	94726	67553	22193
16895	31581	38625	95054	31760	70712	36972	11656	71783	57416	07310
16896	53719	27121	98412	82098	40072	61147	32451	00690	83473	74224
16897	51734	69015	10409	40169	30340	87977	23533	63761	86369	79563
16898	78085	22653	96833	32045	46873	50102	92414	89897	97494	47529
16899	55093	00717	30171	40134	84579	83985	73283	01874	53339	18821

16900	25332	26718	34371	88054	86571	73478	16284	02587	22632	49971
16901	74125	63878	62461	97700	85648	77945	45938	29687	84670	78942
16902	01242	89212	09406	00805	27040	88349	44212	50771	90802	61844
16903	87211	88979	30871	42152	66203	70042	20061	53303	83833	56055
16904	99234	01805	45968	51687	90510	68644	37801	93993	01582	30518
16905	40746	01986	21367	08836	20769	41922	00942	66958	23396	15179
16906	24721	70747	39288	55537	43789	14763	62121	95101	58731	19242
16907	92266	71948	72155	77906	97614	71391	32732	35174	30051	77022
16908	74694	95394	17888	81692	86792	65238	42213	23398	91036	54574
16909	52416	03438	44596	33646	10381	84556	50472	50740	35319	30296
16910	81207	59017	63439	68594	31557	74216	84924	96216	65668	83454
16911	50024	77973	37215	15317	29627	06296	96124	55171	80151	44481
16912	18570	28827	78396	43240	17224	45981	06678	81875	30469	99142
16913	20691	32627	35801	23684	69732	70960	51639	86304	41947	08067
16914	85335	27321	42201	37768	63889	53600	17937	17356	80823	71697
16915	25903	52768	08732	21795	21741	29862	08352	82046	84754	43423
16916	21618	52678	27782	26434	61535	81543	06911	44126	66259	32488
16917	35480	76486	04346	58586	86336	61404	22280	75605	90585	66989
16918	86683	23437	67517	51046	52570	11244	07739	61841	39524	30022
16919	72515	93576	42242	82876	71525	00014	21422	79154	85360	43334
16920	92252	57535	15295	52671	13826	96554	15538	71169	41268	54695
16921	40280	84925	11760	83940	45039	61589	02723	53540	63597	40970
16922	54595	47500	28761	86341	56366	57608	50126	35551	76807	48574
16923	65900	40014	20702	74043	41930	52508	57067	86302	64481	57487
16924	32157	58884	66731	59986	38545	10157	57307	41029	40857	26550
16925	13813	47377	67050	90055	84059	84390	09573	03425	27576	98740
16926	55094	06585	69963	57374	80526	96919	34279	86832	62851	26113
16927	53556	56885	62536	13859	28555	78700	95054	09370	76196	59073
16928	05198	72410	78138	97625	12301	07712	29668	48008	85578	54050
16929	14436	37840	51353	06903	32177	15044	85421	20263	88008	85040
16930	65863	52813	52201	62777	44572	34206	45156	02711	85947	06379
16931	88320	91171	10402	59848	01731	10876	22520	71151	63853	47204
16932	20006	49554	17142	26825	58467	62843	25656	78488	20145	35658
16933	75979	14537	13147	18267	42679	03307	40686	79355	16422	01176
16934	15091	32091	40299	39059	32760	04256	92318	95046	60792	99926
16935	58310	81804	67381	49251	04211	56900	37625	92200	78225	85174
16936	72418	67302	78900	76165	54547	14111	81738	73274	73888	46168
16937	71447	90271	39086	70240	01839	43877	01495	44891	83608	88175
16938	41054	15353	10798	29693	90608	06626	78064	22429	83693	60651
16939	19310	81134	01074	51272	79023	61301	25300	66449	26528	52421
16940	48045	30498	55460	40274	96722	00450	14345	55213	61085	42394
16941	66815	49510	29346	13253	31819	66985	77625	63285	27152	61483
16942	25193	43541	21058	04659	92280	64552	80553	00579	46853	08290
16943	67210	67363	99708	29072	69682	60138	02165	55094	85487	33922
16944	93113	27851	85285	07986	14739	40665	82510	36835	82211	08654
16945	70139	39001	16654	18577	92801	93288	09472	82413	06917	91142
16946	66416	54480	34802	32983	22782	55904	95053	46836	45107	71694
16947	99285	98566	97983	18465	93344	62089	99582	28809	60834	71476
16948	68236	39084	17929	91439	53087	79235	05482	90623	22031	48070
16949	87042	31148	01679	46784	83210	88483	82740	09254	75967	28785