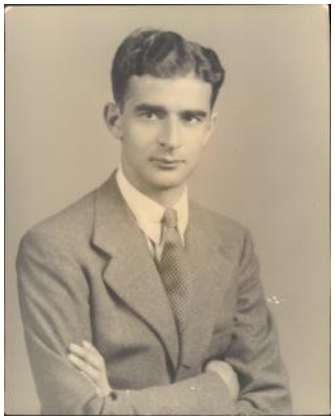
Creativity in Computer Science – Horst Feistel



- Horst Feistel is the son Richard and Helene Feistel of Frankfurt/Oder (Germany); Horst Feistel born in (East) Berlin on January 30, 2015.
- Anecdotal information (?) about Feistel found in Levy's *Crypto*[1].
- Adolf Hitler declares universal military service in 1935.
- Horst's aunt Gertrude in Zurich married to Franz Meyer, a Swiss Jew.
- Telex to Horst ``… come to Zurich to attend to your very ill aunt."
- Horst goes to Zurich (193?) and attends (??) school.
- Horst immigrates to U.S. in 1934; `house arrest' in Cambridge (MA) [1940 census].
- B.S. (Physics) MIT in 1937; M.A. (Physics) Harvard 1942.
- Horst granted citizenship, clearance and job; MIT Rad Lab in 1944 at Hanscom AF Base.
- Horst works at Air Force Cambridge Research Center (AFCRC) in 1945.
- Member at Lincoln Lab staff (1958-61); moves then to MITRE (MIT Computer Science).
- Horst joins the Computer Science Department (IBM Research Center) in 1968.
- Horst switches to Mathematical Sciences Department (IBM Research Center) in 1971.
- Horst retires from IBM to Cape Cod and passes away on November 14, 1990.

---

[1] Steven Levy. ``Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age", Viking, 2001.

Horst Feistel's Work before Employment at the IBM Research Center

Works at the MIT Radiation Laboratory, Air Force Cambridge Research Center (AFCRC) and MIT Lincoln Laboratory on IFF (*Identification Friend or Foe*)[2, 3] project.

A Mode 4 IFF *challenge*[4] sent to an aircraft requires a *valid* IFF response or else 

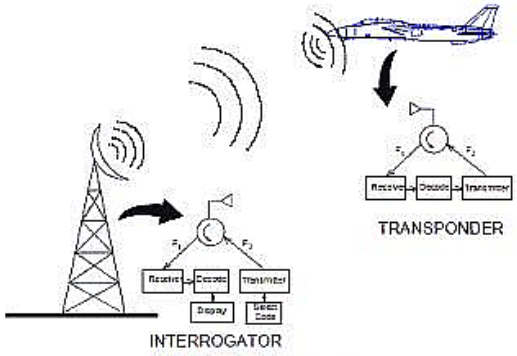
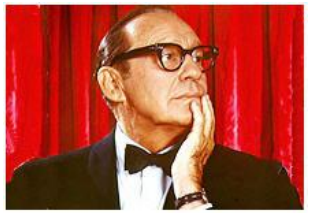


Figure 1. IFF Transponder



Challenge: ``Your wallet or your life?"

Response: ``Wait…I'm thinking!"

Mode 4 IFF *challenge* X $\Rightarrow$ *response* **E**{X,**A,ID**}[altitude (A), aircraft identifier (ID)]

---

[2] Horst Feistel, A Survey of Problems in Authenticated Communication and Control, MIT Lincoln Laboratory, May 20 1958, pp. 1-111.

[3]. Identification, friend or foe (IFF) is an identification system designed for command and control. It enables military and national (civilian air traffic control) interrogation systems to identify aircraft, vehicles or forces as friendly and to determine their bearing and range from the interrogator.

[4] The challenges are `randomly' chosen similar to SSL and TSL key generation protocol.

I AM 10 IN 1944 - UNAVAILABLE TO TEACH CS178

In my place ??? A[3] ≡ A. Adrian Albert[5].

[A[3]'s daughter] Nancy E. Albert's book[6] published in 2005 consists of her reminiscences of the career of A. A. Albert in World War II and after in the area of cryptography.

Ms. Albert's book begins with the statement attributed to David Kahn[7] [p. 410]

> ``A. Adrian Albert was perhaps the first to observe that, as he put it, all of these methods [of cryptography] are very special cases of the so-called algebraic[8] cipher systems.''

---

[5]Abraham Adrian Albert was an American mathematician. He received the American Mathematical Society's Cole Prize in Algebra in 1939 for his work on Riemann matrices and was president of the AMS during 1965-6. As an applied mathematician, he worked for the military during and after World War II. The manuscript, "Some Mathematical Aspects of Cryptography" is a printed version of his invited address at a meeting of the AMS in November 1941 (Z103.A33, University of Chicago Library).

[6]Nancy E. Albert, ``A[3]: His Algebra: How a Boy from Chicago's West Side Became a Force in American Mathematics'', New York, iUniverse, 2005.

[7] David Kahn, ``The Codebreakers (The Story of Secret Writing)," The MacMillan Company, 1967

[8]Examples of algebraic systems include groups, semi-group, rings, ideals, fields. How can the cycle structure of a 19th and 20th century electro-mechanical [algebraic] cipher machine be used for cryptanalysis?

Interaction between A. Adrian Albert and Horst Feistel

Daniel Gorenstein[9] wrote

> ``In the summer of 1957, Horst Feistel's group of cryptanalysts at AFCRC sponsored a research project on classified and unclassified cryptanalytic problems at Bowdoin College. Albert, who had a longstanding interest in cryptanalysis and was a consultant to Feistel's group, invited a distinguished group of university algebraists to participate including I. N. ``Yitz'' Herstein[10], Irving Kaplansky, Irwin Kleinfield, Richard Schafer, and George Seligman. In preparation for the project, Feistel's group prepared a long list of classified and unclassified problems. Although many of these were of a field-theoretic or combinatorial character, under Sy Hayden's influence they included a number of purely group-theoretic questions related to a type of cryptographic system then under investigation."

[9]This is contained in a paper about the classification of the finite simple groups; Gorenstein went on to become one of the leading contributors to Group Theory.

[10] I might have missed joining the early launching of the crypto-boat; while I was a graduate student at Cornell University during 1957-60, Professor Gorenstein was a visitor as were Walter Feit and Itz Herstein. Professor Herstein was a member of my examining committee.

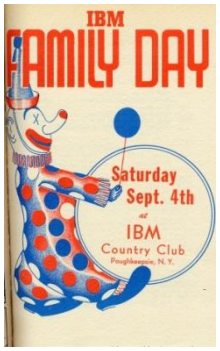
Albert Advises Horst Feistel, ``Go South Young Man to …"

Nancy Albert writes

`` [Albert] was well acquainted with Horst Feistel and having consulted in private industry and served with some of the leaders of industry on various boards, Adrian knew where the jobs were in mathematics. He advised the young Horst Feistel, who felt his interest in exploring cryptography was being stifled at the National Security Agency, to seek employment at IBM. Feistel later flourished in IBM's intellectual playground[11], developing ways to protect privacy in cyberspace.''

Up, up, up and away… oops!

Third trumpet from Stage front



A casualty of Microsoft

[11] Traversing the sides of the stone sides of the IBM Kitchawan Research Center.

A. Adrian Albert's Version of CMPSC 178

Shannon's 1949 paper ``The Theory of Secrecy Systems"[12]

``The problems of cryptography and secrecy systems furnish an interesting application of communication theory. In this paper a theory of secrecy systems is developed."

Perfect secrecy is defined by requiring encipherment to result in

$$P_{a\ posteriori}(M/C) = P_{a\ priori}(M).$$

- $P_{a\ posteriori}(M/C)$: *a posteriori* probability of plaintext M *given* ciphertext C
- $P_{a\ priori}(M)$: *a priori* probability of the plaintext M

An *idea system* is one in which

$H_C(K)$ and $H_C(M)$ do not approach zero as $N \to \infty$

[H is *entropy;* M is *message*; K is *key*; C is *ciphertext*]

[12] *Bell System Technical Journal,* (**28**)4, October 1949, pp. 656-715. Published September 1, 1945 as a classified paper.

Building Blocks of Shannon's Ideal Systems

``Two methods (other than recourse to ideal systems) suggest themselves for frustrating a statistical analysis. "

Diffusion

`` In the method of *diffusion* the statistical structure of M which leads to its redundancy is dissipated into long-range statistics."

Confusion

``The method of *confusion* is to make the relation between the simple statistics of C and the simple description of K a very complex and involved one."

Mixing Transformations [Section 25 of Shannon's Paper]

``Speaking loosely, however, we can think of a mixing transformation as one, which distributes any reasonably cohesive region in the space uniformly over the entire space. Good mixing transformations are often formed by repeated products of two [or more] simple non-commuting operations."

Examples of Confusion, Diffusion and Mixing

- Shannon's example of diffusion $\underline{m} = (m_0, m_1, \ldots, m_{n-1})$ [plaintext]
  [ciphertext] $\underline{c} = (c_0, c_1, \ldots, c_{n-1})$ $c_i = (k_i m_i + k_{i+1} m_{i+1} + \ldots + k_{i+s-1} m_{i+s-1}) \pmod{26}$
- The Hill Cipher[13] cited by Shannon is an example of diffusion.
- Shannon's definition of diffusion suggests it might be achieved by a general permutation of the bits of plaintext bits (*wire crossing*). Each key and plaintext bit affects many bits of the ciphertext.
  - for example, a DES P-box.
- Shannon's definition of confusion suggests it might be achieved by a general substitution of the plaintext symbols. Each bit of the ciphertext is a complex function of the plaintext and key bits.
  - for example, a DES S-box.
- Shannon's definition of mixing suggests it might be achieved by iteration of simpler [low dimensional] confusion and diffusion transformations.
  - for example, multiple rounds of `LUCIFER`, DES and AES

[13] In classical cryptography, the Hill cipher is a polyalphabetic substitution based on linear algebra $C = K M$ where the key K is an n-by-n matrix and M is an n-vector. Invented by Lester S. Hill in 1929, it was the first practical polyalphabetic cipher to encipher more than three symbols at once.

Horst Feistel's Work at IBM

1. He wrote programs in APL[14] (*A Programming Language*).
2. IBM files several patents based on his cryptographic ideas.
   a. Block Cipher Cryptographic System, US#3798359A [filed June 30, 1971];
   b. Key Controlled Block-Cipher Cryptographic System Employing a Multidirectional Shift Matrix, US# 4195200A [filed June 30, 1976];
   c. Stream/Block Cipher Cryptographic System, US#4316055A [filed December 30, 1976]
3. Horst originally chooses `DEMONSTRATION` as name of his block cipher APL program.
   - Early versions of APL limit the character length of the names of APL programs
   - `DEMON` became its truncated name; Horst realized that `LUCIFER` was a sexier choice.

---

[14] APL is a programming language developed in the 1960s by Kenneth E. Iverson.

Rho, rho, rho of X
Always equals 1
Rho is dimension, rho rho rank.
APL is fun!
Richard Stallman

APL was an important influence on the development of spreadsheets, functional programming and computer math packages (MatLab). I taught CS5 (APL) twice at the UCSB Micro Lab on Apple computers. It might have also inspired several other programming languages (Matlab, Mathematica)

I taught CS5 (APL) at the MCL twice at UCSB.

Both 32-and 64-bit GNU APL are available for Windows, truly proving G_d is great! هلّك برال

IBM Enters the Crypto Business (1966)

- IBM 2984 (Cash Issuing Terminal)
  - *Lloyds Bank Cashpoint System*
  - ATM is operational in Essex, England (1972).
- IBM Program Product management at IBM SCD in Kingston

  Kingston proposes Hill polyalphabetic substitution to provide the relationship between PIN and PAN in ATM transaction.

  + Potentially large key space size;
  - Linear encryption is susceptible to a (partial) known *plaintext* attack.
- Walter Tuchman, the IBM project manager realizes weakness of Hill
  - DSD-1 successor to modified `LUCIFER` used in the IBM 2984[15].
  - DSD-1 becomes DES[16] (FIPS 46-1; 11/1976)

---

[15]Hardware implementation: ~ ¼ by ¼ inch, 2 micron CMOS, containing one DES-engine and enciphering at the rate of 4 Mb/s (64 bits in 16 microseconds).

[16] In addition to Feistel's Block Cipher patent, IBM was issued US #3,962,539 ``Product Block Cipher System for Data Security'' describing the design of DES. It was filed by IBM Kingston on June 28, 1976. Listed as inventors were William Friedrich Ehrsam, Carl H. W. Meyer, Robert Lowell Powers, John Lynn Smith and Walter Leonard Tuchman.

But First --- IBM Needs Consultants like a ...

- Professors Edward Glazer[17] from Case Western;
- James Simons SUNY Stony Brook[18] and IDA/CRD [founded in 1959[19]].

Simons `LUCIFER` *Report Excerpt:* ``… no attack, which would recover key from arbitrary amounts of matched plaintext and ciphertext, was *found*. Neither was an attack discovered that would enable one to read a significant fraction of messages without a work factor comparable to that of trial and error."

- Neither Simons nor Glazer found any *attack* or the *alleged backdoor*.
- Arne Beurling's Swedish Cone of Silence (National Defense Radio Establishment (FRA))

  Professor Beurling reverse-engineered a version of the German fish machine [Siemens and Halske T52 *Geheimschreiber*] and developed a cryptanalysis for it.

---

[17]I am cited on page 48 in Levy's ``Crypto' as the source of Glazer's unsubstantiated claim that he could *break* `LUCIFER` with 20 pairs of corresponding plaintext and ciphertext!

[18]In 1982, Simons founded Renaissance Technologies, a private hedge fund investment company based in New York with over $15 billion under management. Simons retired at the end of 2009 as CEO of one of the world's most successful hedge fund companies. Simons' net worth is estimated to be $12.5 billion!

[19]Nancy Albert claims in her book that IDA began earlier in 1956 and was an outgrowth of the Bowdoin College meeting sponsored by Cambridge AFCRC. During 1961-62, A. A. Albert took a leave of absence and served as the first director of IDA/CRD. IDA sought the skills of American mathematicians by sponsoring the SCAMP (Summer Conference on Applied Mathematics Problems); the word *Problems* means those related to the cryptography area.

IBM Patent Protection

IBM Sets U.S. Patent Record
Achieves 21st Straight Year of Patent Leadership
IBM inventors received more than 6,800 U.S. patents in 2013

- Both a United States and European applications made sense as the banking application originated in England with Lloyds Bank Group.
- The Invention Secrecy Act of 1951 (Public Law 82–256, 66 Stat. 3) *prevents* disclosure of new technologies that … a possible *threat* to the national security of the United States.
- *United States Patent Office Rule*: File patent first in the US and reviewed by the Patent Office before foreign patent may be filed. [20]
- *Secrecy Orders*: In cases where the publication… would be detrimental to national security … the Commissioner of Patents may issue a *secrecy order* to stop the patent process. If no secrecy order is issued in the six months after the submission of a U.S. patent application, then … free to file outside United States.
- IBM Science Advisory Committee meeting(May 1973)
  - IBM would create a single cryptographic architecture and
  - *Cryptanalytic* competence center, ``adequate technical contention in cryptography.''
- Secrecy order issued on October 17, 1973; rescinded on November 14, 1973.

[20] 35 U.S.C. 184 Filing of application in foreign country.

The IBM NSA Conflict

i) Need to protect the national security by not revealing to America's many adversaries new cryptographic technology.

ii) Potential significant business opportunities for IBM[21].

- IBM is an international corporation, but has always practiced the quintessential American value - *patriotism.* 
- NSA and IBM had to reach a satisfactory accommodation satisfactory to *both* parties to resolve the conflict.
- IBM SCD Kingston people advised NSA about the chip constraints and advised by them about the secrecy of design principles.

[21]The March 27, 2003 article in Bloomberg News by Bernardo Batiz-Lazlo, `How the ATM Business Revolutionized Banking," summarizes the history of ATMs in banking. It claims the explosion in banking is due in part to the use of dial-up connections replacing dedicated lines making ATMs more economical.

The Compromise

-  NSA wanted to have DES modified to include a *backdoor* to make deciphering DES-ciphertext feasible.
- No one has *discovered* (or has publically revealed) any backdoor.
- The 56-bit DES key size *might* have been the deal breaker[22].
- Secrecy of DES design criteria (T-Attack).
- Smart people run NSA and it took many years before they realized the silliness and futility of the key-size limitation.
- The Export Control Act limited the export of products containing cryptographic utilities with key length of more than 40 bits before the 56-bit DES was approved. All key length restrictions removed in January 2000; products using DES and AES were exportable to all except to the *evil empire!*

---

[22]Walt Tuchman wrote in email that the key size resulted from the chip constraints. He believes that NSA wanted to keep secret the designed criteria. IBM Research discovered T-attack (rediscovered in 1990 by Eli Bilham ``Differential Cryptanalysis'' and by Mitsuru Matsui in 1993 ``Linear Cryptanalysis''. The T-attack and all of IBM''s design criteria were published in 1994,

Don Coppersmith, ``The Data Encryption Standard (DES) and its Strength against Attacks,'' *IBM Journal of Research and Development*, **38**(3), pp. 243-250, May 1994.

Commercial Application Areas of Cryptography

- The IBM-NSA dispute related to banking

  Use cryptography during an ATM transaction to *authenticate* **a user** at a secured location (a bank/supermarket).

  - ATMs now ubiquitous throughout the world; they represent the *first* major successful commercial application of encipherment.
  - Yahoo Finance (April 2014): China for the first time exceeded the United States as the country with the largest number of ATMs.

- In E-Commerce

  Use cryptography during a session to *authenticate* over the insecure Internet, *the* ***seller*** *to the* ***buyer***; additional tools needed were not available in 1971.

What Horst Feistel Did NOT Do?

1. Horst did **not** invent *public key cryptography* (PKC)[23].

- W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, **IT-22**,pp. 644–654, 1976.
  - C. C. Cocks, "A Note on Non-Secret Encryption", CESG Report, 20 November 1973.
  - J. H. Ellis, "The Possibility of Secure Non-Secret Digital Encryption", CESG Report, Jan. 1970.

2. Horst did **not** formulate the *ATM PIN-PAN Protocol or ATM Bankcard Standard*.

- The PIN-PAN protocol used in ATM transactions is described in

U.S. Patent Number 3,543,994 (Geoffrey Ernest Patrick Constable; Smith Industries). Implemented by Chubb Integrated Systems in May 1968 in England.

- American National Standards Institute, "The ANSI Standard X9.1-1980.

---

[23] The *classified* paper of Cocks and Ellis discovered PKC who worked for the Government Communications Headquarters (GCHQ). This is the intelligence and security agency responsible for providing signals intelligence (SIGINT) and information assurance to the British government and armed forces. Their papers were declassified in 1997. GCHQ did not realize the significance of the Internet and public key cryptography commercial applications

Whit Diffie did realize the applicability of PKC, but he did not have any real example of a public key system, although Donald Knuth had suggested factorization as an example of a *one-way function*. D&H did not pursue and PKCs had to wait until the publication in 1978 of RSA.

R. Rivest, A. Shamir and L. Adelman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM***21** (2), pp. 120–126, 1978.

3. Horst did **not** invent the principles of message *authentication*.[24]

- ITU, CCITT, Recommendation X.509, "The Directory – Authentication Framework", Consultation Committee, International Telephone and Telegraph, International Telecommunication Union, Geneva, 1989.

4. Horst did **not** invent the *Secure Socket Layer Protocol*.

- RFC524, ''Transport Layer Security (TLS) Protocol" [Version 1.2] RTF Incorporated, 2008.

[24] Authentication in IFF.

Horst Feistel, ``A Survey of Problems in Authenticated Communication and Control, " MIT Lincoln Laboratory, pp. 1-111, May 20, 1958.

What Horst Feistel Did Achieve?

1. He invented the first of several strong 20th century cipher algorithms.
2. DES (a commercial version of `LUCIFER`) approved as a Federal Information Processing Standard (FIPS) in 1976. Reluctantly reaffirmed as a standard several times; in 1993 affirmation included the statement

   > At the next review (1998), the algorithm specified in this standard will be over twenty years old. NIST will consider alternatives, which offer a higher level of security. One of these alternatives may be propose d new standard at the 1998 review.

3. *Rijndael* the successor to DES announced as the winning algorithm in 2000; augmented and designated as the *Advanced Encryption Standard* (AES) (2001).
4. Cryptographic Encryption prior to DES - electro-mechanical machines[25]
   - Electro-mechanical machines imply some algebraic structure in the encipherment.
   - Starting point in their cryptanalysis; *Enigma* machine [$x \rightarrow y \neq x$].
   - Weak session key protocol of the *Enigma*.

[25]Cipher A. Deavours and Louis Kruh, `Machine Cryptography and Modern Cryptanalysis", Artech House, 1985.

5. New 1971+ crypto algorithms differed from the 19th and 20th century cipher machines.

   LUCIFER, DES and AES were *only* the first of a class of Shannon-inspired (diffusion, confusion, mixing) encipherment systems.

6. The two major missions of NSA are *Information Assurance* (IA) and *Signals Intelligence* (SIGINT); IA protects our country's communications, SIGINT (*aka* COMSEC) is described on a NSA website ---

   `` … collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and ..."

Edgar Allan Poe's story *The Gold Bug* Poe contains the oft-quoted statement

``Yet it may be roundly asserted that human ingenuity cannot concoct a cipher that human ingenuity cannot solve"

Horst's Achievement: Poe's statement may *not* remain accurate today; it may be too (time) costly for NSA to decipher messages encrypted with DES, DES3, AES or subsequent commercial or ***intelligence agency*** successors of these algorithms.

7. NSA is forced to make use of *trapdoor* (or *backdoor*)[26] attacks in place of cryptanalysis to fulfill its SIGINT mission

- Entry by FBI and U.S. Naval Intelligence (OP-20-GY) into the Japanese consulate in Manhattan in 1941 to photograph codebooks.
- The 1958 agreement between the eminent and retired cryptographer William Friedman and Boris Hagelin, the CEO of the Swiss firm *Crypto AG*. It permitted NSA to secretly include NSA-supplied backdoors in cryptographic equipment. Crypto AG sold this doctored equipment to some of their clients, various governments unfriendly to the U.S. through 1992.

8. Horst provided the impetus setting into motion the investigations and technology that led inexorably to today's E-Commerce!

[26]In a legitimate theatre, a *trapdoor* is a sliding or hinged door, flush with the surface of a floor, roof, or ceiling, or in the stage of a theatre. The door is used to make people appear or disappear in a puff of smoke, which hides the closing or opening of the door. In cryptography, it is *an alteration of the enciphering program*, which allows the trapdoor inserter's agents to read messages without the sender's knowledge.

COMPARING SHANNON AND FEISTEL

- Shannon universally considered a giant in technology.
  - Boolean algebra (switching circuit design) [Master's thesis[27]]
  - Mathematical Theory of Communications[28] [Coding Theorem]
  - The Theory of Secrecy Systems[29]

All modern communications [space, navigation (GPS) and the Internet]

Feasible implementation of research spawned by Shannon's 1948 paper.

- Horst Feistel was inventive, but certainly not in the same technical league with Shannon. However …
  - ATM technology and **all** of the advantages of E-commerce are the products of groundbreaking work spawned by Horst Feistel's research.

---

[27] ``A Symbolic Analysis of Relay and Switching Circuits," *Transactions AIEE,* **57**(12): 713–723, 1938.

[28] ``A Mathematical Theory of Communication", *Bell System Technical Journal,* (**27**)3, July 1948, pp. 379-423.

[29] ``The Theory of Secrecy Systems," *Bell System Technical Journal*, October 1949, (**28**)4: 656-715,

- *State Street* downtown Santa Barbara, California.
  - Stores open, flourish and disappear ---
    Remaining are banks, bars, national chain stores, restaurants and coffee shops.
    Gone are locally owned small businesses.
- *Amazon*.com, USPS, UPS and FedEx are E-Commerce winners.
- Is E-Commerce a *blessing* or a *curse*?
- Is E-Commerce a similar achievement worth celebrating?
- Does the technology derived from research of Feistel compare to that of Shannon?

I am not percipient enough to give an answer … I am only a (former) line-editor-using retired Professor of Computer Science!