Ramping up to World War II

Chris Christensen
Northern Kentucky University
1976 The Diffie-Hellman paper

Whitfield Diffie  

Martin Hellman
<table>
<thead>
<tr>
<th>Mathematician/cryptologist</th>
<th>Girolamo Cardano</th>
<th>François Viète</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(1501 – 1576)</td>
<td>(1540 – 1603)</td>
</tr>
</tbody>
</table>
Charles Dodgson (1832 – 1898)
Lester S. Hill (1891 - 1961)
Bletchley Park

- Alan Turing
- I J Good
- Philip Hall
- Peter Hilton
- David Rees
- Max Newman
- J.H.C. Whitehead
- Shaun Wylie
- Gordon Welchman
William Wray (1910 – 1962)
1999 inductee to the NSA/CSS Hall of Honor.

1924 Safford reported to the newly established Cryptographic Research Desk in naval communications.

July 1924 section of the monthly bulletin devoted to cryptanalysis.
Correspondence course
Naval Security Station (October, 1945)
Howard T. Engstrom (1902 – 1962)
Row 3, Person 5

- Ph.D. in mathematics from Yale in 1929.
- 1931 studied at Gottingen.
- Was an associate professor of mathematics at Yale when he recruited mathematicians to serve with the Navy.
- Commanded OP-20-G Research Section.
- After World War II, co-founded Engineering Research Associates (ERA) that delivered the first Atlas computer to the Navy in 1950. The commercial version of Atlas was Univac.
- 1957 – 1958 Deputy director of research and development for NSA. Then deputy director of NSA.
- After leaving NSA was vice president of Sperry Rand.
Andrew Gleason (1921 – 2008)

Row 2, Person 5

- Bachelor’s degree in mathematics from Yale in 1942 and began service with the Navy.
- After World War II was appointed a Junior Fellow at Harvard. He never received a Ph.D.
- Known for his work on Hilbert’s Fifth Problem.
- 1969 appointed Hollis Professor of Mathematicks and Natural Philosophy (the oldest endowed scientific position in the US). 27 Ph.D. students
Marshall Hall, Jr. (1910 – 1990)
Row 2, Person 2

- Studied for a year in England with Philip Hall, Harold Davenport, and G. H. Hardy – 1933.
- Ph.D. from Yale 1936; student of Oystein Ore.
- One year at the Institute for Advanced Study and then accepted a position at Yale.
- Taught at Yale until service with the Navy.
Alfred Clifford (1908 – 1992)
Row 3, Person 1

- 1933 Ph.D. from Cal Tech; student of Eric Temple Bell.
- Institute for Advanced Study where he served for five years as assistant to Herman Weyl – while Weyl was writing *The Theory of Classical Groups*.
- Taught at MIT from 1938 – 1942.
- Johns Hopkins after World War II.
- 1950 – 1952 returned to duty for the Korean War.
- Beginning 1955, Tulane.
More mathematicians

- Robert Greenwood (1911 – 1993) Row 3, person 4
  Ph.D. from Princeton (1939). Advisor was Salomon Bochner. Academic career at University of Texas except for (1950 – 1952) service during the Korean War. 10 Ph.D. students.

- Eugene Hanson Row 3, person 6
  Ph.D. from OSU in 1936. 1935 – 1957 chair of the Department of Mathematics as University of North Texas.
William Blankinship (1922 – 1998) Row 3, person 12. Bachelor’s degree Virginia (1941); Ph.D. Princeton (1949); 2005 inductee to NSA Hall of Honor: “pioneering research in mathematical applications to cryptography and was a pioneer in computer programming.”

“The work did not really need mathematics but mathematicians tended to be good at it.”
“The quality that was principally required of us at Bletchley was really the ability to think mathematically. ... we could have done nothing had we not had the experience of really getting down to some piece of work, of achieving a deep analysis and executing it.”
A. A. Albert (1905 – 1972)

“... cryptography is more than a subject permitting mathematical formulation, for indeed it would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics.”

November 22, 1941
SCAMP: Southern California Applied Mathematics Project

- “Albert was the primary proponent of the SCAMP project that was held each summer in California – at UCLA.”
- About 30 mathematicians working on problems selected by the NSA.

- A. A. Albert
- Andrew Gleason
- J. Barkley Rosser
- John Thompson
- Irving Kaplansky
- John Milnor
- Donald Knuth
Papers by A. A. Albert for the NSA

Author: Albert A A
Title: Reaction normal matrices satisfying the incidence equation
CCR Log #: 8421
Date Written: 08/08/1955

Author: Albert A A
Title: Some smaller properties of the incidence equation
CCR Log #: 8490
Date Written: 22/07/1955

Author: Albert A A
Title: On proper solutions of the incidence equation
CCR Log #: 8467
Date Written: 11/09/1955

Author: Albert A A
Title: A note on linear recursive relations
CCR Log #: 8476
Date Written: 07/08/1955

Author: Albert A A
Title: On products of linear recursive sequences
CCR Log #: 8475
Date Written: 08/07/1955

Author: Albert A A
Title: On product of recursively generated sequences
CCR Log #: 8454
Date Written: 09/08/1955

Author: Albert A A
Title: Some remarks on trinomial equations
CCR Log #: 8456
Date Written: 10/08/1955

Author: Albert A A
Title: A note on non-linear recursive sequences
CCR Log #: 8496
Date Written: 10/07/1956

Author: Albert A A
Title: Some properties of recursive sequences
CCR Log #: 8512
Date Written: 19/06/1956

Author: Albert A A
Title: Linear spans of maximal cycles
CCR Log #: 8513
Date Written: 31/08/1956

Author: Albert A A
Title: Solution of scan problem No. 9
CCR Log #: 8511
Date Written: 16/07/1957

Author: Albert A A
Title: Two-signal generation of a unimodular group
CCR Log #: 8592
Date Written: 01/09/1957

Author: Albert A A
Title: Report to the director of the air force cambridge research center on the 7th summer mathematical conference
CCR Log #: 8490
Date Written: 03/09/1957

Author: Albert A A
Title: On norms in cyclotomic rings II
CCR Log #: 8689
Date Written: 12/01/1958

Author: Albert A A
Title: On certain norms in cyclotomic rings I
CCR Log #: 80314
Date Written: 12/01/1958

Author: Albert A A
Title: Generation of a finite field by a unit
CCR Log #: 8552
Date Written: 02/02/1959

Author: Albert A A
Title: On complete mappings
CCR Log #: 83692.112
Date Written: 02/09/1959

Author: Albert A A
Title: On complete mappings
CCR Log #: 83692.112
Date Written: 02/09/1959

Author: Albert A A
Title: On complete mappings
CCR Log #: 8569
Date Written: 02/02/1960

Author: Albert A A
Title: On complete mappings
CCR Log #: 8354
Date Written: 01/10/1960

Author: Albert A A
Title: On a class of trinomial equations
CCR Log #: 8575
Date Written: 03/08/1961

Author: Albert A A
Title: On certain trinomial equations in finite fields
CCR Log #: 80632.163
Date Written: 01/01/1964

Author: Albert A A
Title: On certain trinomial equations in finite fields
CCR Log #: 80624.163
Date Written: 02/01/1964
Topics

- Linear recursive sequences.
- Trinomial equations in finite fields.
- Generation of a unimodular group.
- Norms in cyclotomic rings.
- Complete mappings.
- Trinomial equations in finite fields.
- Construction of irreducible polynomials.
- Algebraic theories over a finite field of characteristic 2.
Fundamental Concepts of Higher Algebra (1956)

- Groups
- Rings and fields
- Vector spaces and matrices
- Theory of algebraic extensions
- Finite fields

“The preparation of this text was supported by the Department of Defense. The author acknowledges the very kind assistance of Drs. W. A. Blankinship and E. C. Paige ... .”
“... I believe that it is safe to say that Albert had more influence in the post war development of cryptology in the U.S. than any other mathematician in the U.S.”
Albert was “undoubtedly very instrumental in persuading the U.S. government to establish the National Security Agency.”
Largest employer of mathematicians in the world?