

# Crypto in Central Europe

Nicolas T. Courtois

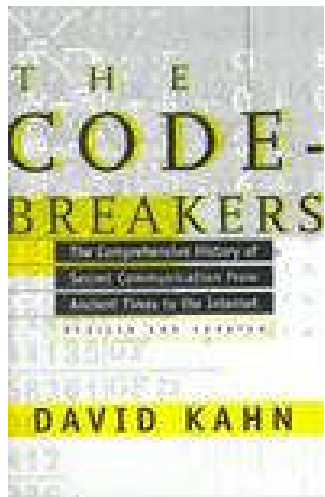
University College London, UK

# Marian Rejewski

December 1932:

$$26! \approx 2^{88.4}$$

reverse engineering of Enigma rotors



- “the greatest breakthrough in cryptanalysis in a thousand years” [David Kahn]
- cf. John Lawrence, "A Study of Rejewski's Equations", Cryptologia, 29 (3), July 2005, pp. 233–247.  
non-commutative  $P.Q \neq Q.P$

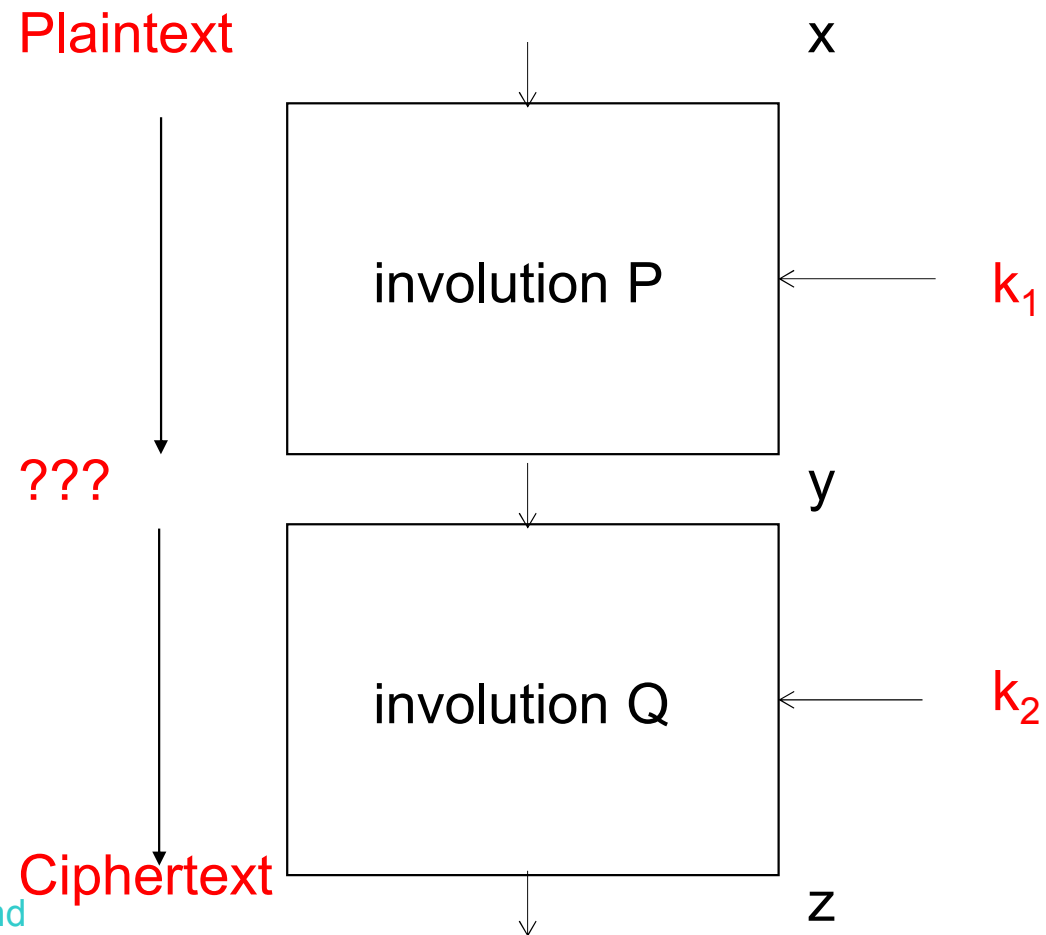
$$AD = CPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}C^{-1}$$

factoring permutations!

# Factoring Permutations

quite surprising  
used in breaking Enigma prior to 1938!

## Key Recovery?



# Factoring Permutations – Miracle!

**Fact 20 (Rejewski Permutation Factoring Method).** Let  $Q \circ \mathcal{P}$  be a composition of two involutions, and let  $\mathcal{P}$  have  $p$  rounds and let  $Q$  have  $q$  rounds with  $p \leq q$ . We assume that the attacker has oracle access to  $Q \circ \mathcal{P}$ . We assume that there is a key recovery attack on  $\mathcal{P}$  given the fact that it has only  $p$  rounds, and that this attack requires only a limited number of P/C pairs. Then attacker can factor  $Q \circ \mathcal{P}$  and recover the key of  $\mathcal{P}$ .

## Proof:

*Justification:* We apply Fact 19 above and consider the smallest value  $k$  such that  $Q \circ \mathcal{P}$  has exactly 2 cycles of length  $k$ , which following Fact 19 must be related and one cycle is  $X, Q(\mathcal{P}(X)), \dots$  the other is  $\mathcal{P}(X), \mathcal{P}(Q(\mathcal{P}(X))), \dots$  possibly starting at some location inside the other cycle. We just need to guess which cycle is which, pick a random point on once cycle, and guess which point on the second cycle is the corresponding points. Overall with probability  $\frac{1}{2k}$  we obtain as many as  $k$  correct P/C pairs for  $\mathcal{P}$  which should be sufficient for key recovery.

# Zygalski “Netz” Attack on Enigma



Zygalski

fixed points for  $R_1 \circ R_4$

Stacking them allowed to  
determine the key uniquely...

attributed by Turing to himself(!)

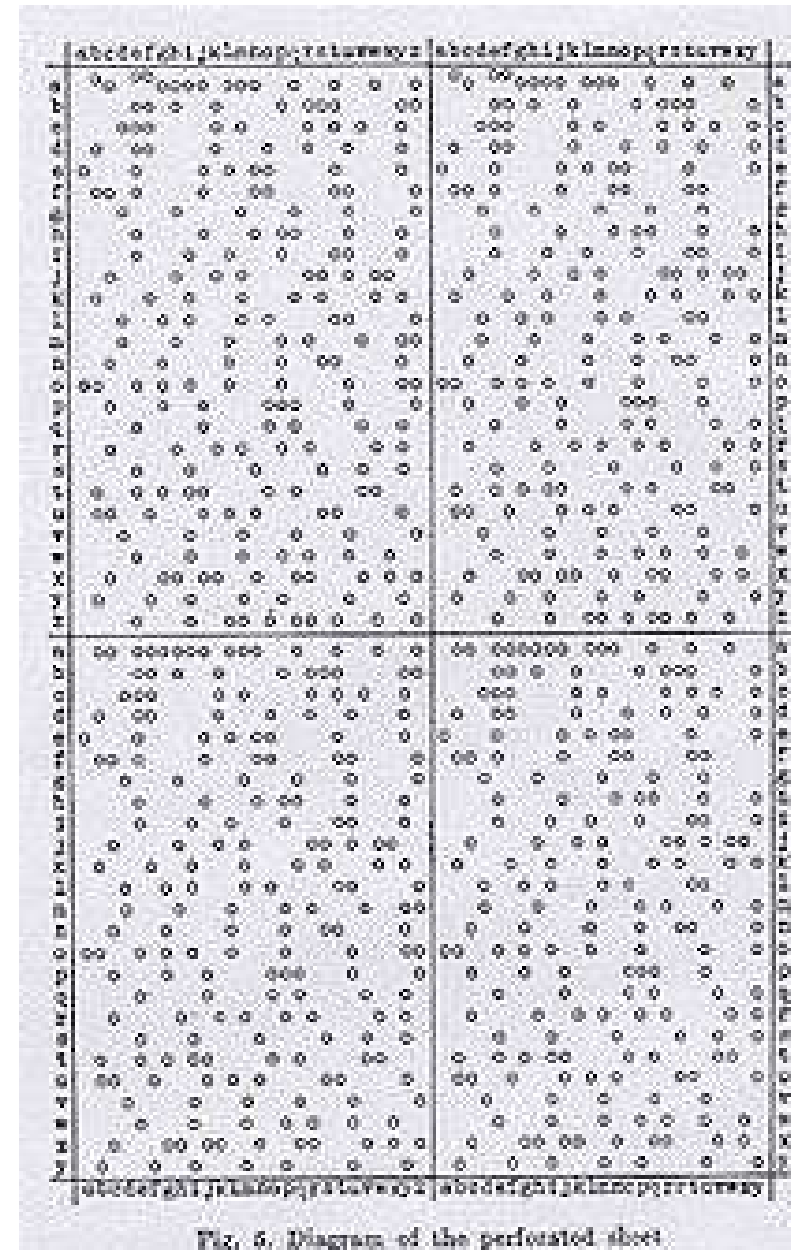
The truth:

=>panic at Bletchley Park: no single message broken

=> chief UK cryptologist (Dilly) wrote a letter saying  
that he will quit if they do not let Turing travel to  
France

=>delivered by Turing in person during his visit to  
France 17 Jan 1940

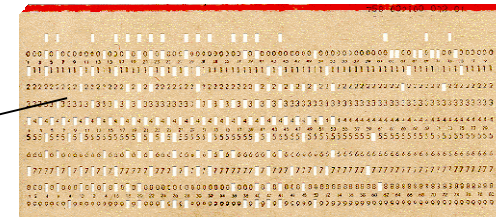
Bugs or Backdoors?  
Nicolas T. Courtois, 2012



# East German SKS V/1 and T-310



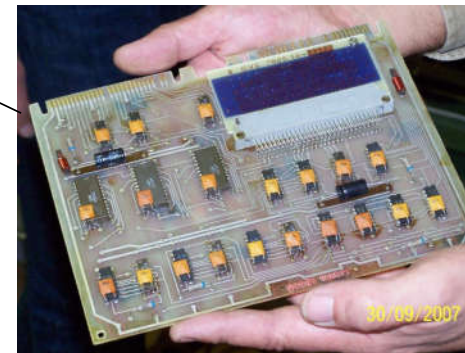
T-310



240 bits

“quasi-absolute security”  
[1973-1990]

designed by Eastern German mathematicians  
with training/advice from Soviet Union

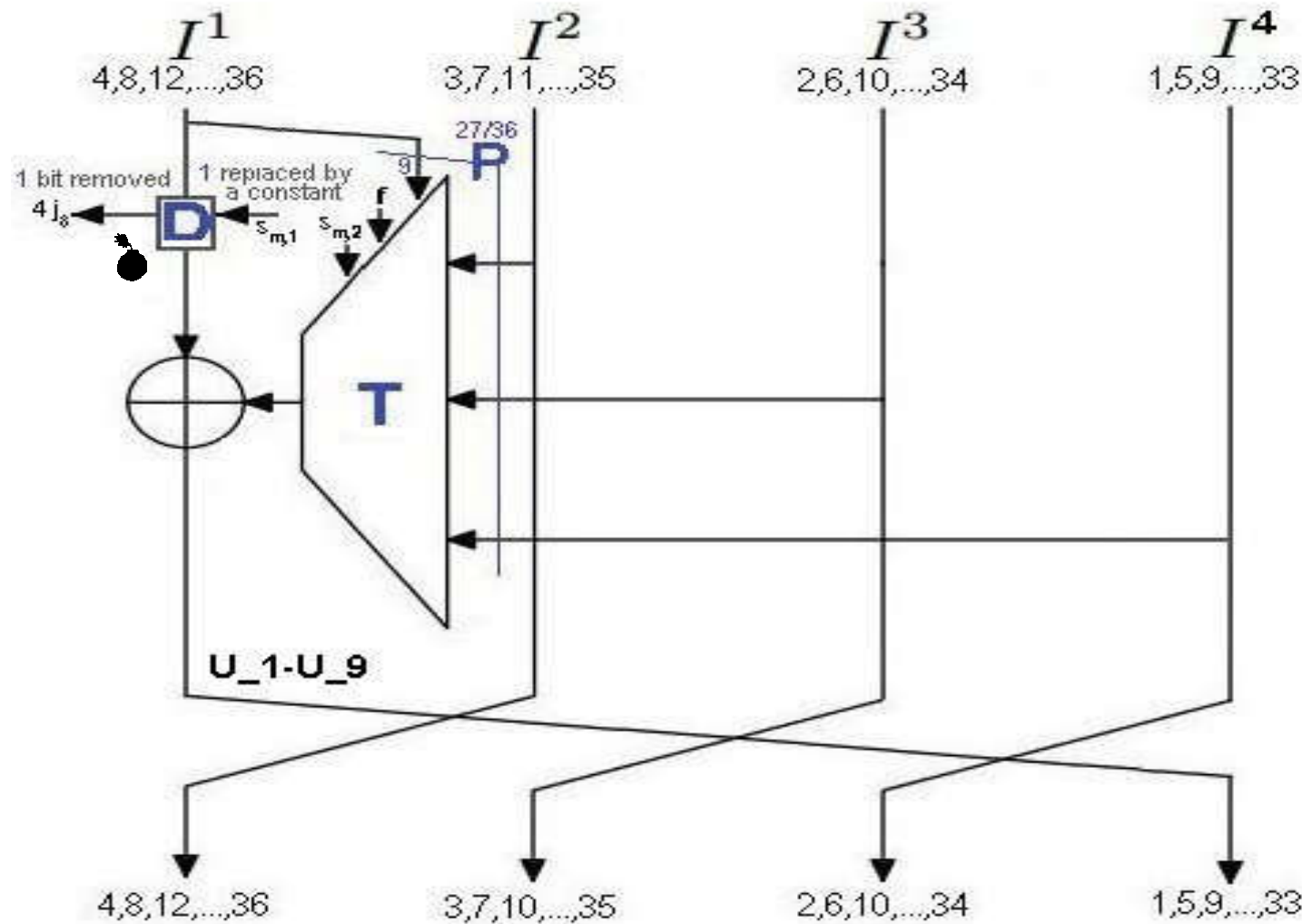


very high  
side-channel security!

long-term secret  
90 bits only!



# Sophisticated/Very Complex Generalized Feistel - before 1975!



very substantial  
complexity EVEN by  
today's standards



# Simple Method to Backdoor T-310 [Courtois 2017]

1,3,5 => 1,3,5

P=1

703

P=7,14,33,23,18,36,5,2,9,

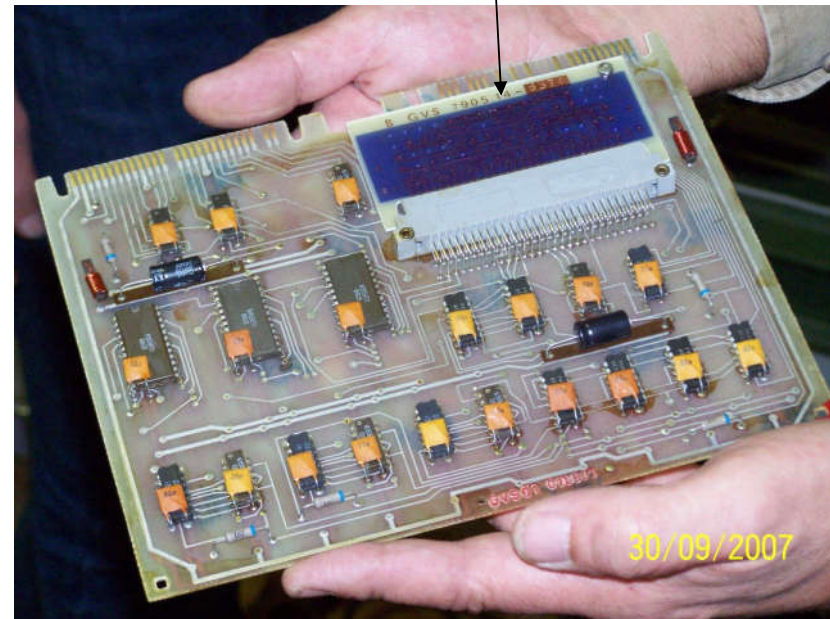
16,30,12,32,26,21,1,13,25,

20,8,24,15,22,29,10,28,6

D=0,4,24,12,16,32,28,36,20



bad long-term key



# How to Backdoor T-310 [to appear in 2017]

omit just 1 out of 40 conditions:

ciphertext-only

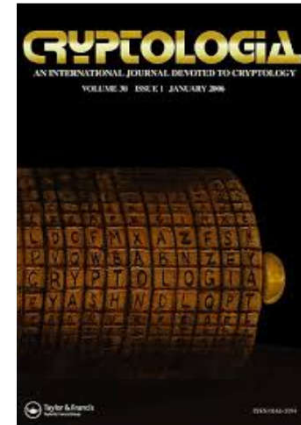
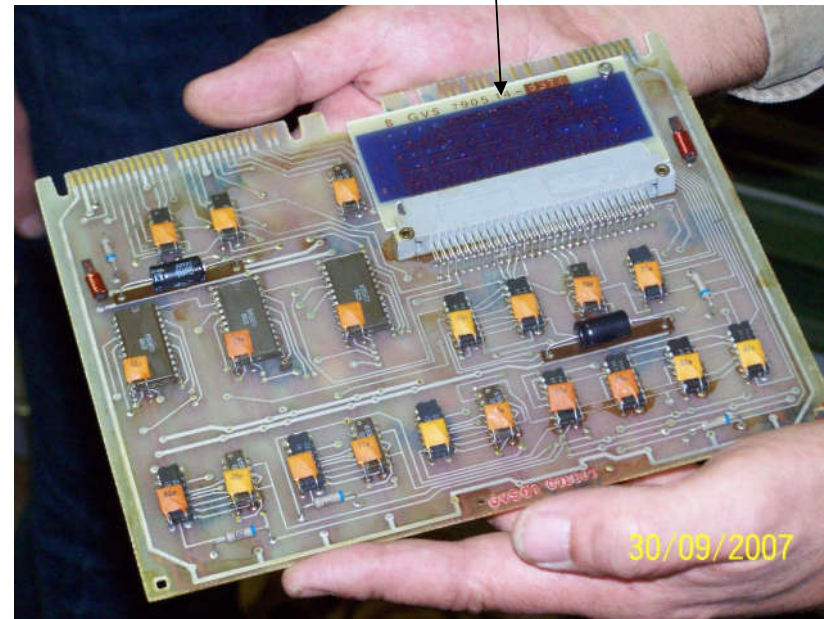
bad long-term key

Lots of constraints

=>

90 bits only!

$D$  and  $P$  are injective  
 $P(3) = 33, P(7) = 5, P(9) = 9, P(15) = 21, P(18) = 25, P(24) = 29$   
 Let  $W = \{5, 9, 21, 25, 29, 33\}$   
 $\forall_{i \geq 9} D(i) \notin W$   
 $\alpha \notin W$   
 Let  $T = (\{0, 1, \dots, 12\} \setminus W) \cap (\{P(1), P(2), \dots, P(24)\} \cup \{D(4), D(5), \dots, D(9)\} \cup \{\alpha\})$   
 Let  $U = (\{13, \dots, 36\} \setminus W) \cap (\{P(26), P(27)\} \cup \{D(1), D(2), D(3)\})$   
 $|T \setminus \{P(25)\}| + |U \setminus \{P(25)\}| \leq 12$   
 $A = \{D(1), D(2), D(3), D(4), D(5), D(6), D(7), D(8), D(9)\} \cup \{P(6), P(13), P(20), P(27)\}$   
 $A_1 = \{D(1), D(2)\} \cup \{P(27)\}$   
 $A_2 = \{D(3), D(4)\} \cup \{P(20)\}$   
 $A_3 = \{D(5), D(6)\} \cup \{P(13)\}$   
 $A_4 = \{D(7), D(8)\} \cup \{P(6)\}$   
 $\forall(i, j) \in \{1, \dots, 27\} \times \{1, \dots, 9\} : P_i \neq D_j$   
 $\exists_{\hat{j}} \in \{1, \dots, 7\} : D_{\hat{j}} = 0$   
 $\{D(8), D(9)\} \subset \{4, 8, \dots, 36\} \subset A$   
 $\forall(i, j) \in \{1, 27\} \times \{1, 9\} : P_i \neq D_j$   
 $\exists_{\hat{j}} \in \{1, 7\} : D_{\hat{j}} = 0$   
 $\{D_8, D_9\} \subset \{4, 8, \dots, 36\} \subset A$   
 $\exists(j_2, j_3) \in (\{j \in \{1, 4\} | D_j \neq A_j\})^2 \wedge$   
 $\exists(j_4, j_5) \in (\{1, 4\} \setminus \{j_1, 2j_2 - 1, 2j_2\}) \times (\{5, 8\} \setminus \{j_1, 2j_2 - 1, 2j_2\}) \wedge$   
 $\exists_{j_6} \in \{1, 9\} \setminus \{j_1, 2j_2 - 1, 2j_2, j_4, j_5\} :$   
 $j_2 \neq j_6 \wedge \{4j_4, 4j_5\} \subset A_{j_6} \wedge$   
 $A_{j_6} \cap (4j_1 - 3, 4j_1 \cup 4j_5 - 3, 4j_5) \neq \emptyset \wedge$   
 $\{8j_2 - 5, 8j_2\} \subset A_{j_6} \wedge A_{j_6} \cap (4j_1 - 3, 4j_1 \cup 4j_5 - 3, 4j_5) \neq \emptyset;$   
 $\{D(9)\} \setminus \{33, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(8), D(9), P(1), P(2), \dots, P(5)\} \setminus \{29, 32 \cup \{0\}\} \neq \emptyset$   
 $\{D(7), D(8), P(1), P(2), \dots, P(6)\} \setminus \{25, 32 \cup \{0\}\} \neq \emptyset$   
 $\{D(7), D(9), P(1), P(2), \dots, P(6)\} \setminus \{25, 28 \cup 33, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(6), D(7), D(8), D(9), P(1), P(2), \dots, P(12)\} \setminus \{21, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(5), D(7), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus \{17, 20 \cup 25, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(7), D(8), D(9), P(1), P(2), \dots, P(6)\} \setminus \{25, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(5), D(6), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus \{17, 24 \cup 29, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(5), D(6), D(7), D(9), P(1), P(2), \dots, P(13)\} \setminus \{17, 28 \cup 33, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(5), D(6), D(7), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus \{17, 32 \cup \{0\}\} \neq \emptyset$   
 $\{D(5), D(6), D(7), D(8), D(9), P(1), P(2), \dots, P(13)\} \setminus \{17, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(4), D(5), \dots, D(9), P(1), P(2), \dots, P(19)\} \setminus \{13, 36 \cup \{0\}\} \neq \emptyset$   
 $\{D(3), D(4), \dots, D(9), P(1), P(2), \dots, P(20)\} \setminus \{9, 36 \cup \{0\}\} \neq \emptyset$   
 plus the "Matrix rank = 9 condition"  $M_9$  defined in Section D.4 below.



# Comparison of R&D Expenses in Different Countries in % of GDP

- Mongolia 0.2% Pakistan 0.3%
- Belarus, Bulgaria 0.70% Ukraine, Greece 0.8%
- Poland, Turkey 0.9%
- Brazil, Russia 1.1%
- Portugal 1.4%
- Canada, UK 1.6%, Note: UK gets 1.7 billion / year from the EU.
- Czech Rep. 1.9% China 2.0%
- Australia, France, Belgium, Estonia 2.3%
- Austria 2.7% Germany 2.80%
- Sweden 3.2% Japan 3.4% Finland 3.6%
- Korea 3.8% Israel 4.1%

source: World Bank

Nicolas Courtois blog:

<http://blog.bettercrypto.com/?p=2759>

# Comparison of R&D Expenses in Different Countries

## in % of GDP

- Mongolia 0.2% Pakistan 0.3%
- Belarus, Bulgaria 0.70% Ukraine, Greece 0.8%
- Poland, Turkey 0.9%
- Brazil, Russia 1.1%
- Portugal 1.4%
- Canada, UK 1.6%, Note: UK gets 1.7 billion / year from the EU.
- Czech Rep. 1.9% China 2.0%
- Australia, France, Belgium, Estonia 2.3%
- Austria 2.7% Germany 2.80%
- Sweden 3.2% Japan 3.4% Finland 3.6%
- Korea 3.8% Israel 4.1%

self-inflicted  
misery!!!!

impossible to claim  
there is no money!

source: World Bank

Nicolas Courtois blog:

<http://blog.bettercrypto.com/?p=2759>

# CECC'17 - Central European Crypto Conference

<http://cecc17.tele.pw.edu.pl/>



## 17th Central European Conference on Cryptology

Welcome to CECC'17.

The Central European Conference on Cryptology will be the 17th in the series of meetings gathering the researches involved in cryptology. In 2001 the series was inaugurated with TATRACRYPT '01 held in Liptovský Ján, Slovakia.

CECC'17 will be held on **June 28-30, 2017** in **Warsaw, Poland**.

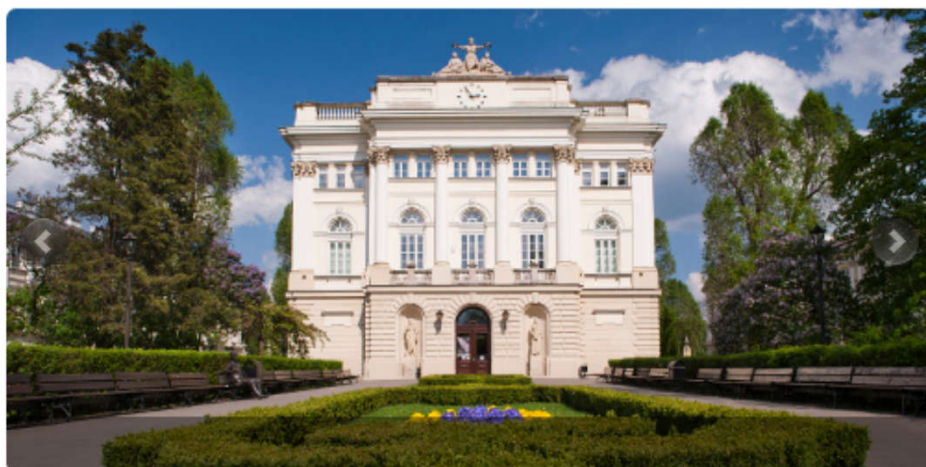
- Short abstract submission: 10 May
- good place for work in progress.
- Conf. in Warsaw 28-30 June
- Final papers will be re-submitted for journal post proceedings paper:
  - theoretical: Fundamenta Informaticae
  - practical: International Journal of Electr. and Telecom.





# Number Theory Methods in Cryptology (NuTMiC)

<http://nutmic.mimuw.edu.pl/>



*Number Theory Methods in Cryptology  
(NuTMiC)*

To be held at the University of Warsaw,  
Warsaw, Poland

September 11-13, 2017

Partners



Organizers



- Short abstract submission: 31 May
- Conf. in Warsaw 11-13 Sept
- Springer LNCS proceedings
  - 30 pages allowed!

# European Historical Ciphers Colloquium 2017

Selected talks:

Thur 09.15

## The Gustave Bertrand Files –

by Dermot Turing

Thur 10.45:

## A General Solution to M-94

by Nils Kopal

Thur 13.30

## German Spy Ciphers of WW2

by Klaus Schmeh

Thur 13.30

## Priceless Gift – Polish Cryptanalysis of Enigma

by Philippe Guillot

Friday 09h00

## History of Public Key Cryptography and RSA

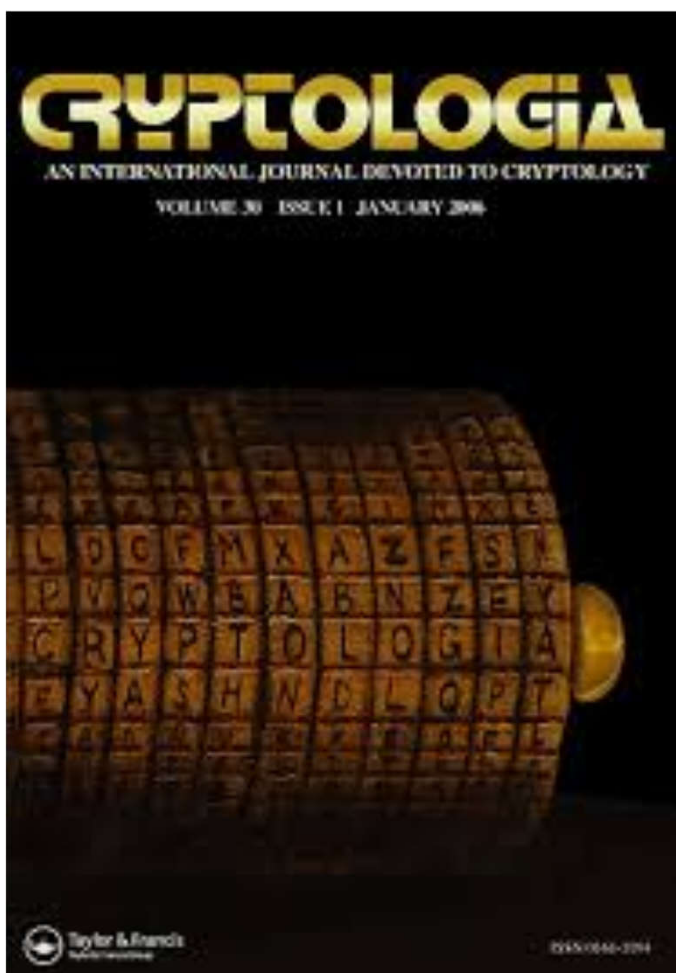
by JJ Quisquater

[euro-hcc.org](http://euro-hcc.org)



- Submission: too late.
- Conf. in Slovakia: **18-19 May**
  - travel from Vienna or Bratislava airport.
- Printed proceedings

Can Still Submit!



# CRYPTOLOGIA

## EDITOR-IN-CHIEF

Craig Bauer  
York, PA, USA  
cryptoauthor@gmail.com

## REVIEW EDITOR

Chris Christensen  
Department of Mathematics  
Northern Kentucky University  
Highland Heights, KY, USA  
christensen@nku.edu

## FOUNDING EDITORS

Cipher A. Deavours  
Department of Mathematics  
Kean University of New Jersey  
Union, NJ, USA  
cdeavours@kean.edu

Brian J. Winkel  
Editor Emeritus  
Dept. of Mathematical Sciences  
United States Military Academy  
West Point, NY, USA  
brianwinkel@hvc.rr.com

## Editorial Assistant

Dante Molle  
Roseto, PA, USA  
dante42.13@gmail.com

David Kahn  
New York, NY, USA  
DavidKahn1@aol.com

Greg Mellen  
Editor Emeritus  
In Memoriam

Louis Kruh  
Editor Emeritus  
In Memoriam

## EDITORIAL BOARD

Kent D. Boldan  
Queens College,  
The City University of  
New York, NY, USA  
boklan@boole.cs.qc.cuny.edu

Whitfield Diffie  
Center for International Security  
and Cooperation,  
Stanford University,  
Stanford, CA, USA  
diffie@stanford.edu

Bob Hanyok  
6500 Walker Branch Dr.  
Laurel, MD, USA  
rjhanyok@verizon.net

David Naccache  
Ecole normale supérieure,  
Département d'informatique,  
Paris, France  
david.naccache@ens.fr

Stephen Budiansky  
Leesburg, VA, USA  
sb@budiansky.com

Ralph Erskine  
Parliament Buildings, Stormont,  
Belfast, Northern Ireland, UK  
erskine\_ralph@yahoo.co.uk

David Hatch  
Center for Cryptologic History,  
National Security Agency,  
Fort Meade, MD, USA  
dahatch@nsa.gov

Raphael C.-W. Phan  
Multimedia University,  
Malaysia  
raphaelphan.crypt@gmail.com

Augusto Buonafalce  
San Terenzo, Italy  
augusto@cdh.it

Wes Freeman  
Mt. View, CA, USA  
wesf@worldnet.att.net

Joshua Brandon Holden  
Department of Mathematics,  
Rose-Hulman Institute  
of Technology,  
Terre Haute, IN, USA  
holden@rose-hulman.edu

Klaus Schmeh  
Gelsenkirchen, Germany  
klaus@schmeh.org

Colin Burke  
Columbia, MD, USA  
burke@umbc.edu

David W. Gaddy  
Tappahannock, VA, USA  
dwgaddy@verizon.net

David Joyner  
Mathematics Department,  
United States Naval Academy  
Annapolis, MD, USA  
wdj@usna.edu

Alan T. Sherman  
Department of Computer  
Science & Electrical Engineering,  
University of Maryland,  
Baltimore County  
Baltimore, MD, USA  
sherman@umbc.edu

Jan Bury  
Cardinal Stefan  
Wyszynski University,  
Warsaw, Poland  
j.bury@uksw.edu.pl

James J. Gillogly  
Los Angeles, CA, USA  
sryer@gmail.com

David Kahn  
Great Neck, NY, USA  
DavidKahn1@aol.com

William Stallings  
USA, ws@shore.net or  
http://williamstallings.com/

Nicolas T. Courtois  
Computer Science,  
University College London,  
London, UK

Lee A. Gladwin

Frode Weierud



# LinkedIn

LinkedIn  Account Type: Basic

[Home](#) [Profile](#) [Contacts](#) [Groups](#) [Jobs](#) [Inbox](#) 2 [Companies](#) [News](#) [More](#)

Your Groups (51) [Reorder](#) »

[+ Create a](#)

    **Code Breakers** **Members (712)**



 **IACR Cryptographers**

