# Crypto
# in Central Europe

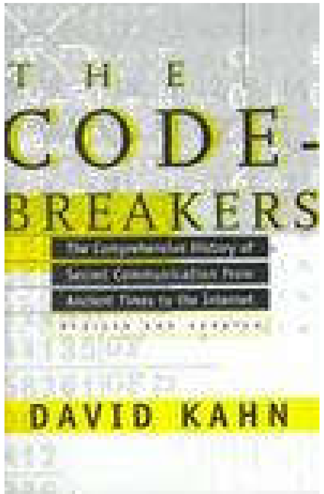
Nicolas T. Courtois

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 ≠ Q.P

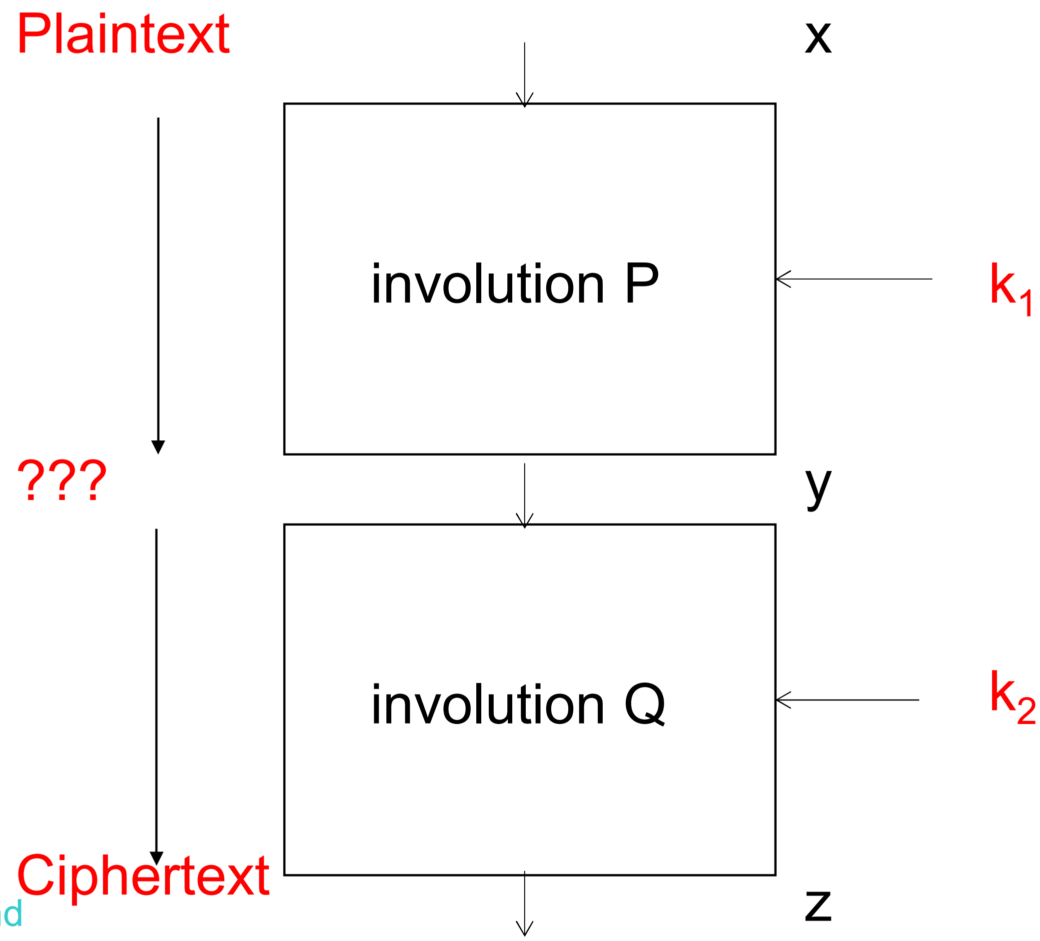
$$AD = CPNP^{-1}QPN^{-1}P^{3}NP^{-4}QP^{4}N^{-1}P^{-4}C^{-1}$$

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 $\mathcal{Q} \circ \mathcal{P}$ be a composition of two involutions, and let $\mathcal{P}$ have $p$ rounds and let $\mathcal{Q}$ have $q$ rounds with $p \leq q$. We assume that the attacker has oracle access to $\mathcal{Q} \circ \mathcal{P}$. 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 $\mathcal{Q} \circ \mathcal{P}$ and recover the key of $\mathcal{P}$.

Proof:

*Justification:* We apply Fact 19 above and consider the smallest value $k$ such that $\mathcal{Q} \circ \mathcal{P}$ has exactly 2 cycles of length $k$, which following Fact 19 must be related and one cycle is $X, \mathcal{Q}(\mathcal{P}(X)), \ldots$ the other is $\mathcal{P}(X), \mathcal{P}(\mathcal{Q}(\mathcal{P}(X))), \ldots$ 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

fixed points for $R_1 \circ R_4$

Stacking them allowed to determine the key uniquely…

Zygalski

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

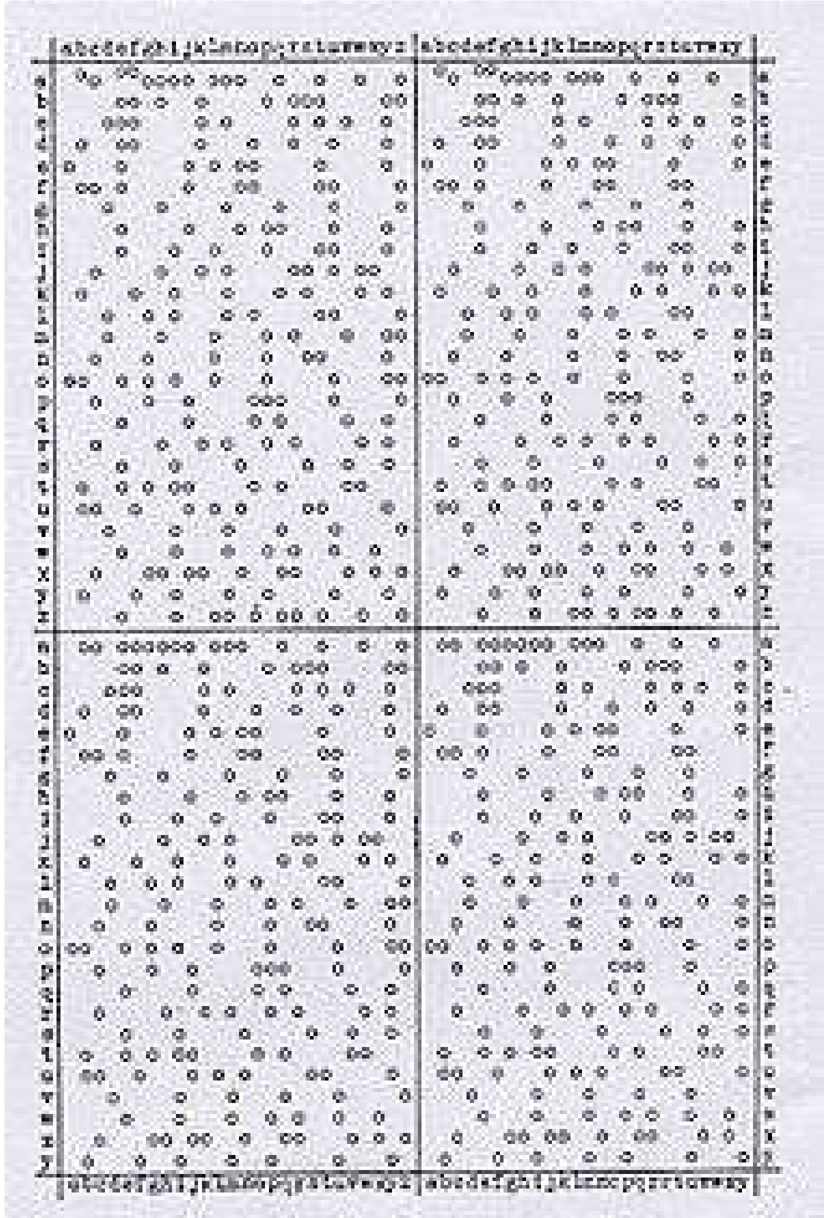
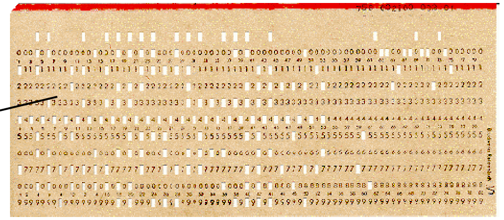


Fig. 6. Diagram of the perforated sheet

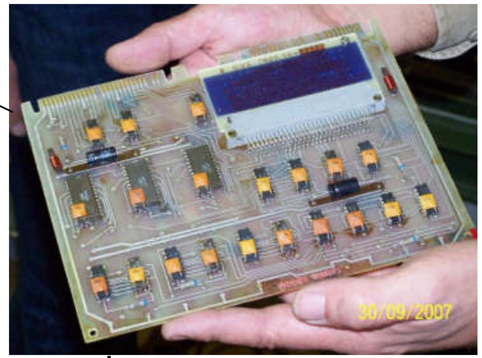
# East German SKS V/1 and T-310

T-310



240 bits

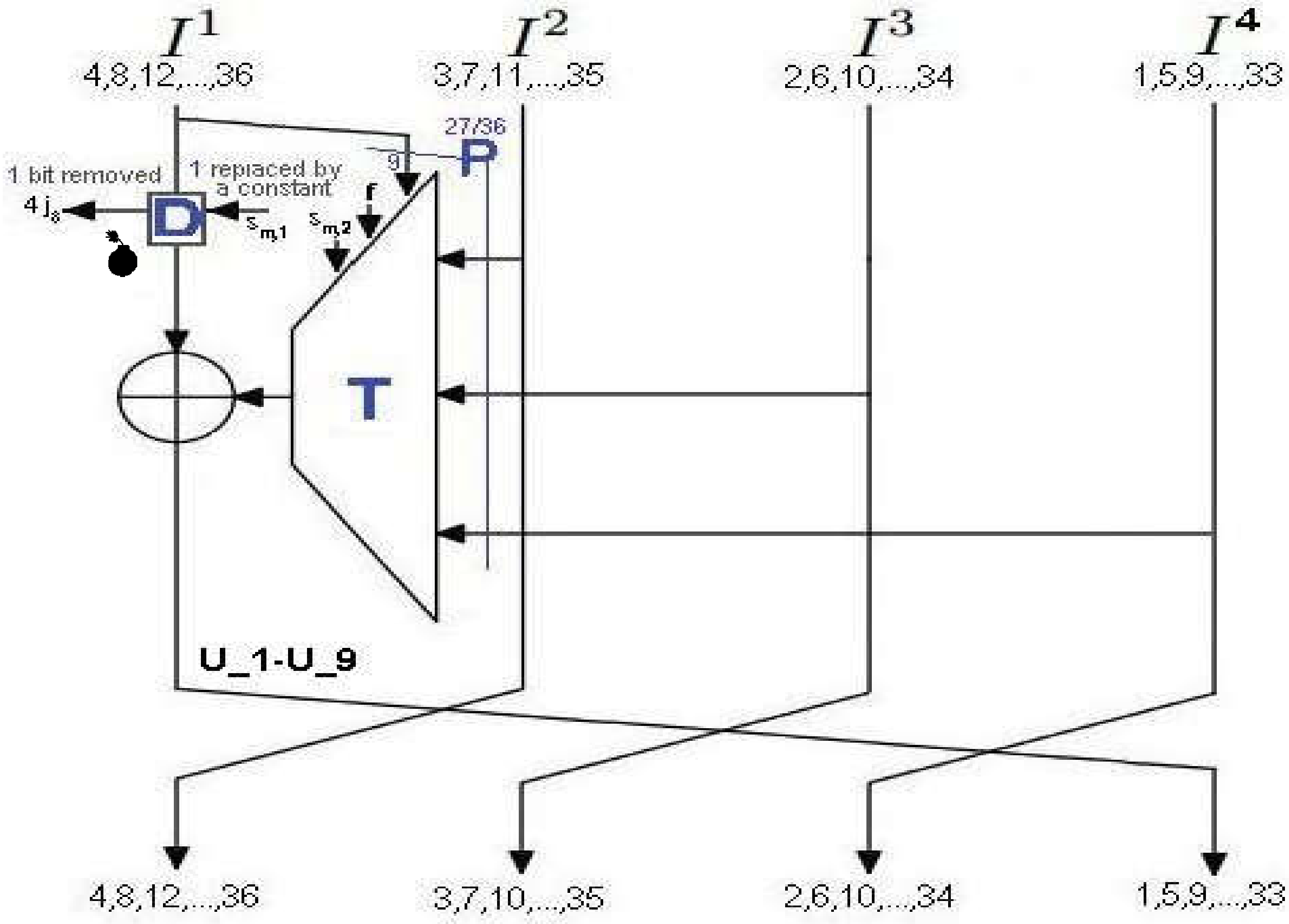
"quasi-absolute security"
[1973-1990]
designed by Eastern German mathematicians
with training/advice from Soviet Union




long-term secret
90 bits only!

very high
side-channel security!

# Sophisticated/Very Complex Generalized Feistel - before 1975!

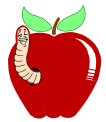



very substantial complexity EVEN by today's standards

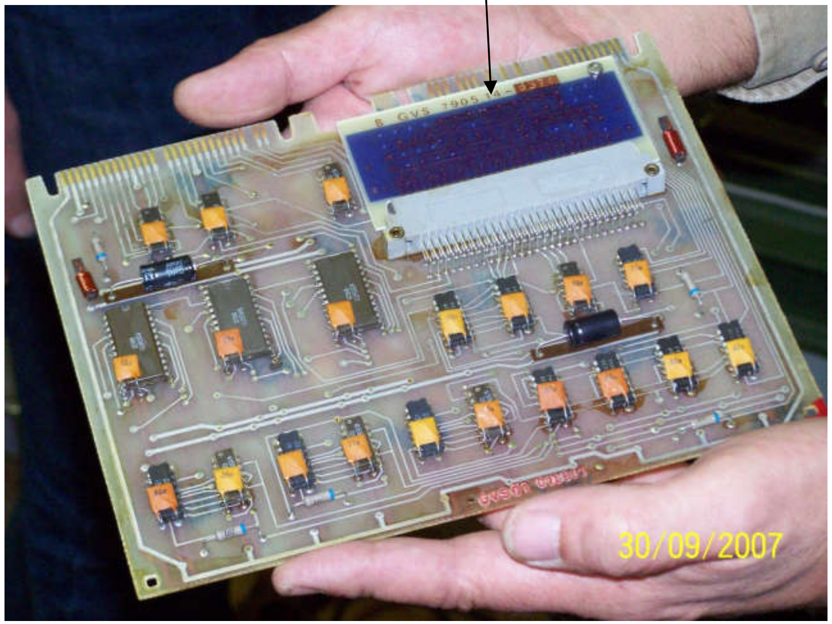
# Simple Method to Backdoor T-310 [Courtois 2017]

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

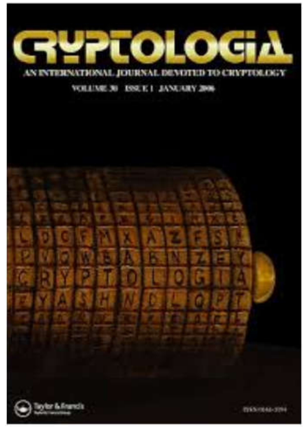
703
P=7,14,33,23,18,36,5,2,9,
16,30,12,32,26,21,1,13,25,
20,8,24,15,22,29,10,28,6
D=0,4,24,12,16,32,28,36,20



bad long-term key



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




omit just 1 out of 40 conditions:

$D$ and $P$ are injective

$$P(3)=33, P(7)=5, P(9)=9, P(15)=21, P(18)=25, P(24)=29$$

$$\text{Let } W=\{5,9,21,25,29,33\}$$

$$\forall_{1\geq i\geq 9} D(i)\notin W$$

$$\alpha \notin W$$

$$\text{Let } T=(\{0,1,\ldots,12\}\backslash W)\cap(\{P(1),P(2),\ldots,P(24)\}\cup\{D(4),D(5),\ldots,D(9)\}\cup\{\alpha\})$$

$$\text{Let } U=(\{13,\ldots,36\}\backslash W)\cap(\{P(26),P(27)\}\cup\{D(1),D(2),D(3)\})$$

$$|T\backslash\{P(25)\}|+|U\backslash\{P(25)\}|\leq 12$$

$$A=\{D(1),D(2),D(3),D(4),D(5),D(6),D(7),D(8),D(9)\}\cup\{P(6),P(13),P(20),P(27)\}$$

$$A_1=\{D(1),D(2)\}\cup\{P(27)\}$$

$$A_2=\{D(3),D(4)\}\cup\{P(20)\}$$

$$A_3=\{D(5),D(6)\}\cup\{P(13)\}$$

$$A_4=\{D(7),D(8)\}\cup\{P(6)\}$$

$$\forall(i,j)\in\{1,\ldots,27\}\times\{1,\ldots,9\}: P_i\neq D_j$$

$$\exists j_1\in\{1,\ldots,7\}: D_{j_1}=0$$

$$\{D(8),D(9)\}\subset\{4,8,\ldots,36\}\subset A$$

$$\forall(i,j)\in\overline{1,27}\times\overline{1,9}: P_i\neq D_j$$

$$\exists j_1\in\overline{1,7}: D_{j_1}=0$$

$$\{D_8,D_9\}\subset\{4,8,\ldots,36\}\subset A$$

$$\exists(j_2,j_3)\in(\{j\in\overline{1,4}|D_j?\notin A_j\})^2\wedge$$

$$\exists(j_4,j_5)\in(\overline{1,4}\backslash\{j_1,2j_2-1,2j_2\})\times(\overline{5,8}\backslash\{j_1,2j_2-1,2j_2\})\wedge$$

$$\exists j_6\in\overline{1,9}\backslash\{j_1,2j_2-1,2j_2,j_4,j_5\}:$$

$$j_2\neq j_3\wedge\{4j_4,4j_5\}\subset A_{j_2}\wedge$$

$$A_{j_2}\cap(\overline{4j_1-3,4j_1}\cup\overline{4j_6-3,4j_6})\neq\emptyset\wedge$$

$$\{8j_2-5,8j_2\}\subset A_{j_3}\wedge A_{j_3}\cap(\overline{4j_1-3,4j_1}\cup\overline{4j_6-3,4j_6})\neq\emptyset;$$

$$\{D(9)\}\backslash(\overline{33,36}\cup\{0\})\neq\emptyset$$

$$\{D(8),D(9),P(1),P(2),\ldots,P(5)\}\backslash(\overline{29,32}\cup\{0\})\neq\emptyset$$

$$\{D(7),D(8),P(1),P(2),\ldots,P(6)\}\backslash(\overline{25,32}\cup\{0\})\neq\emptyset$$

$$\{D(7),D(9),P(1),P(2),\ldots,P(6)\}\backslash(\overline{25,28}\cup\overline{33,36}\cup\{0\})\neq\emptyset$$

$$\{D(6),D(7),D(8),D(9),P(1),P(2),\ldots,P(12)\}\backslash(\overline{21,36}\cup\{0\})\neq\emptyset$$

$$\{D(5),D(7),D(8),D(9),P(1),P(2),\ldots,P(13)\}\backslash(\overline{17,20}\cup\overline{25,36}\cup\{0\})\neq\emptyset$$

$$\{D(7),D(8),D(9),P(1),P(2),\ldots,P(6)\}\backslash(\overline{25,36}\cup\{0\})\neq\emptyset$$

$$\{D(5),D(6),D(8),D(9),P(1),P(2),\ldots,P(13)\}\backslash(\overline{17,24}\cup\overline{29,36}\cup\{0\})\neq\emptyset$$

$$\{D(5),D(6),D(7),D(9),P(1),P(2),\ldots,P(13)\}\backslash(\overline{17,28}\cup\overline{33,36}\cup\{0\})\neq\emptyset$$

$$\{D(5),D(6),D(7),D(8),P(1),P(2),\ldots,P(13)\}\backslash(\overline{17,32}\cup\{0\})\neq\emptyset$$

$$\{D(5),D(6),D(7),D(8),D(9),P(1),P(2),\ldots,P(13)\}\backslash(\overline{17,36}\cup\{0\})\neq\emptyset$$

$$\{D(4),D(5),\ldots,D(9),P(1),P(2),\ldots,P(19)\}\backslash(\overline{13,36}\cup\{0\})\neq\emptyset$$

$$\{D(3),D(4),\ldots,D(9),P(1),P(2),\ldots,P(20)\}\backslash(\overline{9,36}\cup\{0\})\neq\emptyset$$

plus the “Matrix $rank=9$ condition” $M_9$ defined in Section D.4 below.

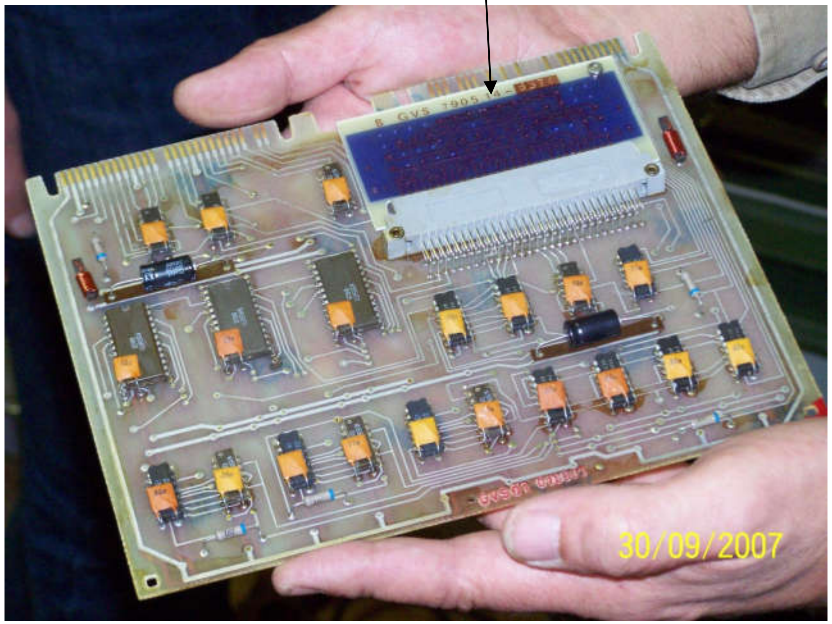
Lots of contraints

=>

90 bits only!

ciphertext-only

bad long-term key



# 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

self-inflicted misery!!!!
impossible to claim there is no money!

- 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

# 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**.

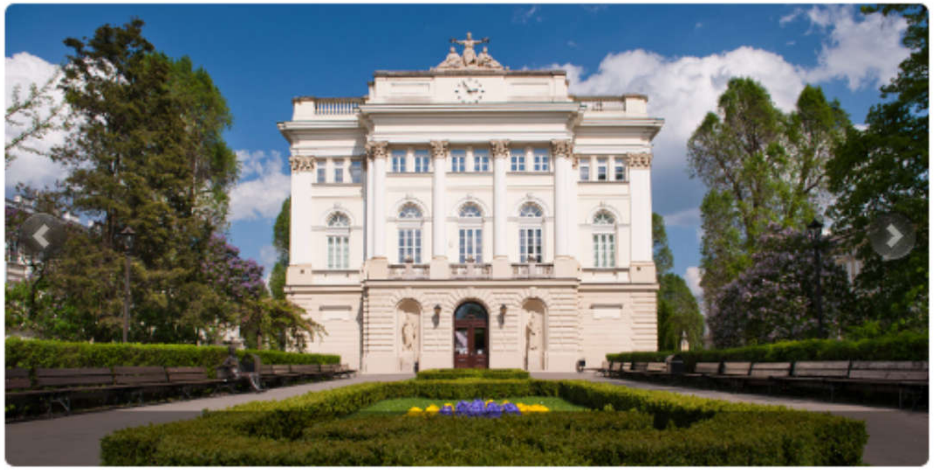
- Short abstract submission: 10 May
- good place for work in progress.

- 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

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

Springer

Organizers

UNIVERSITAS VARSOVIENSIS

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

# European Historical Ciphers Colloquium 2017

[euro-hcc.org](euro-hcc.org)

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

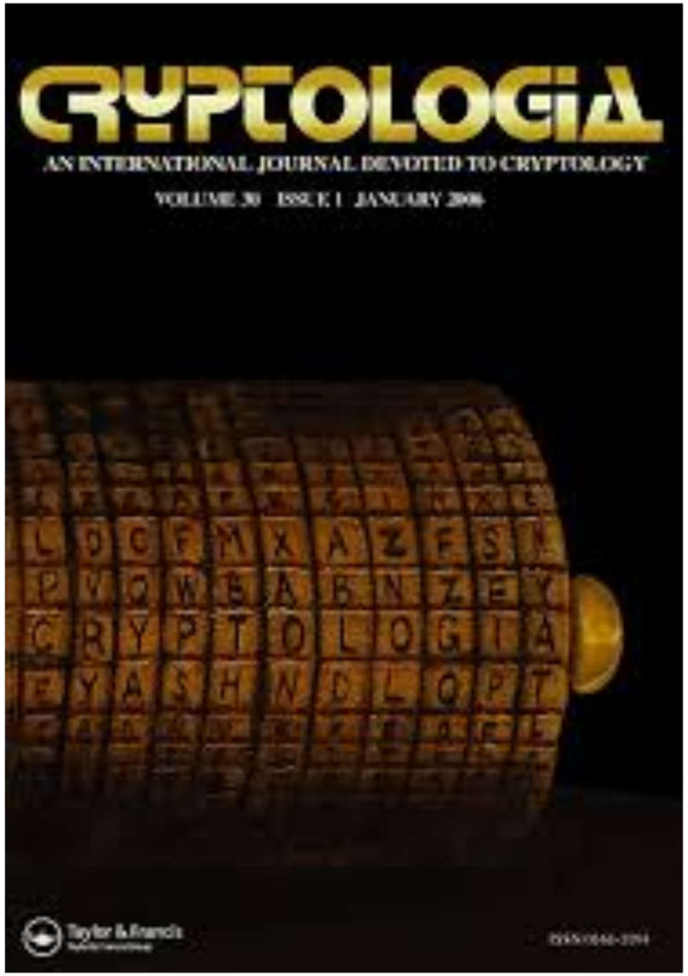
Friday 09h00

History of Public Key Cryptography and RSA

by JJ Quisquater

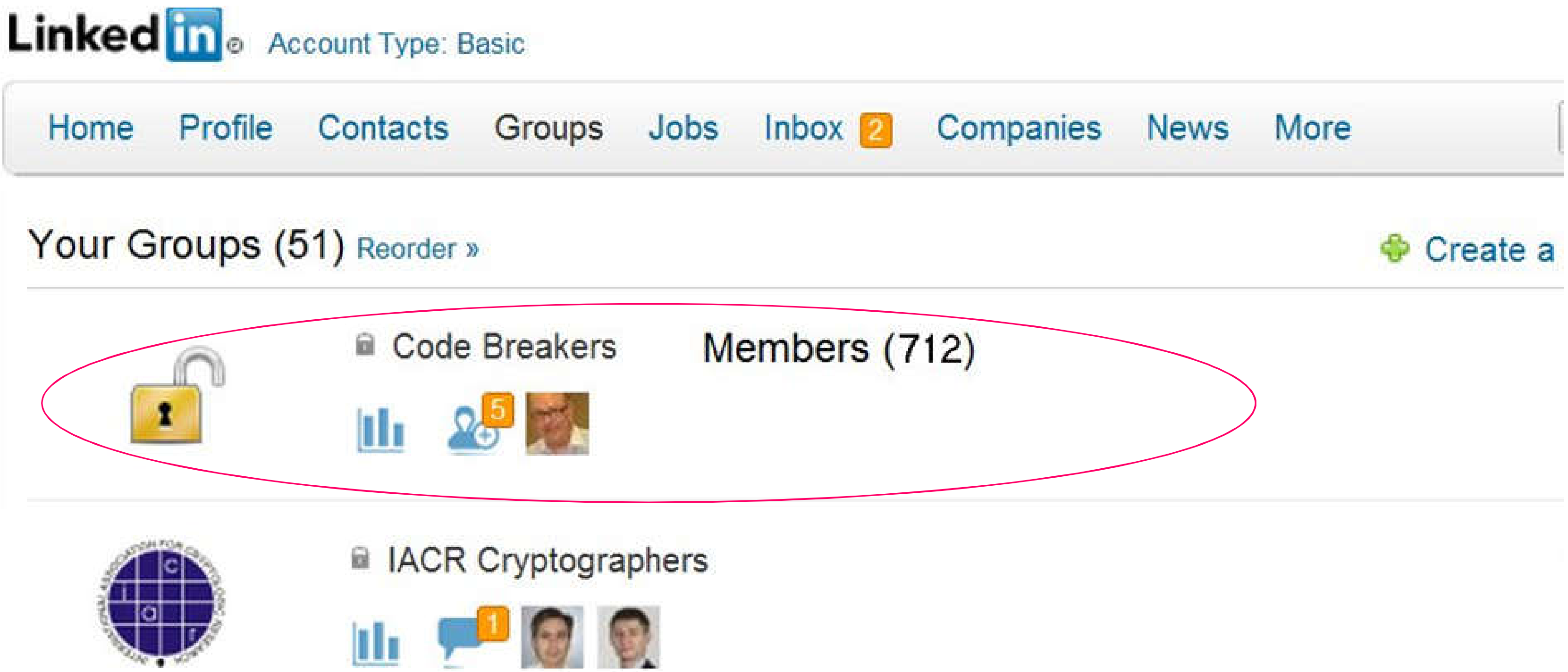
- Submission: too late.
- Conf. in Slovakia: 18-19 May
  - travel from Vienna or Bratislava airport.
- Printed proceedings

# Can Still Submit!




## CRYPTOLOGIA

# LinkedIn


Linked in
Account Type: Basic
Home
Profile
Contacts
Groups
Jobs
Inbox 2
Companies
News
More
Your Groups (51) Reorder »
Create a
Code Breakers
Members (712)
5
IACR Cryptographers
1