



A new ciphertext-only cryptanalysis of the Caesar cipher based on novel semantic-based sampling techniques and application to breaking anonymity of a renowned scientist

Marc Girault

Independent expert

(formerly in France Telecom Orange Labs R&D)

Rue d'Ulm, 4 September 2009



Contents



1. Introduction

2. Dictionary attack (main result)

3. Birthday attack

4. Conclusion





Introduction

- **June 2009** : a popular french dictionary integrates some new entries such as *geek, Web 2.0, Barack Obama, pipolisation, Jane Birkin, moto-taxi*.... and a claimed scientist of claimed name *Jacques Stern*
- **July 2009** : this fact generates an amazing Internet *buzz* (also a new entry), for the famous hacker *Axk Yoltk* conjectures this entry is a *masquerade*
- **September 2009** : we prove the conjecture, by using pretty novel cryptanalytic techniques



Dictionary attack



- Theorem : Under standard assumptions
 - « JACQUES STERN » is a cryptogram
 - The cryptosystem is the Caesar cipher as used by himself when fighting Gaule
 - True identity of so-called « JACQUES STERN » is GXZNRBP PQBOK





Proof (outline)

- Key idea n°1 : JACQUES STERN has the flavour of a pseudonym (concatenation of trivial Christian name and surname)
- Key idea n°2 : the number of letters of JACQUESSTERN is the same as JULIUSCAESAR
- Key idea n°3 : Each initial of the conjectured true name GXZNRBP PQBOK refers to a key feature of this scientist (see below)



Recall :

GXZNRBP PQBOK



G as... GPS



- GPS identification and signature schemes
 - Proved the security with Poupard
 - Variants : PSG, GSP (still room for three)



X as... X !



- The High School he did not enter
 - But gave courses and had several PhD students
- Did he make the good choice ?
 - Theorem : Yes
 - Proof : An X known under exactly the same pseudonym did not enter the dictionary



Z as... Zero-knowledge



- Code-based identification protocol
 - Relies upon general decoding problem
 - One of my favourite papers
- Others
 - CLE (Constrained Linear Equations)
 - GPS (see above)



N as... NTRU



- A famous encryption scheme he *could/should* have designed
 - Strong connection with lattices
 - Light-weight basic operations
- A famous encryption scheme he *could/should* have broken
 - With lattices of course
 - Probably too much beer at Crypto'96 rump session



R as... ROM



(Random Oracle Model)

- Not the inventor but
 - Substantially improved usability with Pointcheval
 - Forking lemma
 - OAEP-RSA
- The model is questionable but
 - Initiated provable security
 - Very useful debugging tool



Bas... Block-Cipher




- He also contributed to symmetric cryptography
 - CS-Cipher with Vaudenay
 - xmx (firmware) with M'Raihi, Naccache and Vaudenay





P as... PRNG

(Pseudo-Random Number Generator)

- **Breaking**
 - PRNG based on truncated linear congruential equations
 - A(nother) wonderful application of lattices
 - One of my favourite papers
 - **Designing**
 - Decoding problem-based PRNG with Fischer
- 

P as... Petit Larousse



- Still to enter
 - Petit Larousse Maxi-Poche (only Isaac)
 - Petit Larousse Poche (only Isaac)
 - Mini-Larousse (a maxi-challenge : not even Isaac)





Q as... Quartier Latin

- Who can imagine him living out of the *berceau* of the French capital ?
 - ...
 - Rue des Ecoles (G. Pompidou...)
 - Rue Saint-Jacques
 - Rue d'Ulm (preferred to rue de la Montagne Sainte-Geneviève)
 - Place Jussieu
 - Rue d'Ulm (again)
 - Rue Descartes
 - Rue Pierre Nicolle
 - ...



B as... Breaker



- He broke a great variety of cryptosystems,
 - alone or
 - with Toffin, Chee, Joux, Girault, Blackburn, Murphy, Coppersmith, Vaudenay, Gentry, Jonsson, Szydlo, JP Stern, Naccache, Smart, Kunz-Jacques, Martinet, Poupard, Dubois, Granboulan, Fouque, Shamir, Macario Rat, Perret, Baignères, ... (sorry for omissions)



O as... Oracle



- One of the two oracles used by Adi Shamir for breaking his schemes
 - Guess the other one ?



(last but not least)



K as... Kissing !

- The dark side of this renowned scientist
- With Gilles Lachaud (who also celebrated his 60th birthday two years ago, in a still nicer place), obliged unfortunate many n -dimensional spheres to stay in a small volume and to kiss a maximum each other



K also as... † Kahn (Gilles)



- The only French name quoted in the CNRS Gold Medal speech, along with Borel, Vigenère, Pompidou and Puvis de Chavannes
- Would also have been a beautiful First Gold Medal in Computer Science



Birthday attack



- Theorem : At half of his life GZNRBP PQBOK met **JXOZ DFOXRIQ** and had some influence on his career
- Proof : 4 September 1979 was the day of first lesson of analysis in the cursus for preparing “agregation” in University of Caen



Conclusion



- As a consequence of the *dictionary attack*, all the Petit Larousse ed. 2010 should be returned to the editor in order to replace the spoofing name by the true name
- As a consequence of the *birthday attack*, cryptology is a disease still more dangerous than H1N1 virus : you can catch it even when the one you shake hand is not yet sick !

