A Distinguishing Attack on Highly-Iterated Ciphers

$\sim\sim\sim$

Gregory V. Bard

joint work with

Nicolas Courtois and Shaun Ault

Highly Iterated Ciphers

- Suppose Alice iterates a cipher 1,000,000 times.
- Bob iterates a cipher 1,081,079 times.
- Charlie iterates a cipher 1,081,080 times.
- There's an attack which can distinguish Charlie (and less so, Alice) from a random cipher, but it fails against Bob?!?!
- Note: $1,081,080 - 1,081,079 = 1$

The Theorem

- Plain English: If you raise a random permutation to a high power k, you can expect $\tau(k)$ fixed points.
- Math: Let π be taken at random from S_n. Let the expected number of fixed points of π^k be e_n. Then
$$\lim_{n\to\infty} e_n = \tau(k)$$
- Reminder: The number of positive integers dividing k is $\tau(k)$.

The Attack

- You are presented with either ($b = 0$) Alice/Bob/Charlie's cipher, or ($b = 1$) a random permutation.
- You can ask for the encryption of some plaintexts, and then you have to guess which one you are presented with (guess the value of b).
- Just sample a small portion of the plaintext space, and see how many fixed points you get!
- $\tau(1,000,000) = 49$; $\tau(1,081,079) = 2$; $\tau(1,081,080) = 256$; $\tau(1) = 1$

Results

- Query 1/64th of the plaintext space.
- If you get a fixed point anywhere in there, guess it is Alice/Bob/Charlie ($b = 0$). If you don't, then guess it is a random permutation ($b = 1$).

	No fixed points	One or more	Target	Success
$k = 1$	0.985041	0.014959	Random	
$k = 1000000$	0.797284	0.202716	Alice	59.39%
$k = 1081079$	0.984409	0.015591	Bob	50.03%
$k = 1081080$	0.418335	0.581665	Charlie	78.34%

Morale of the Story

- If you have to iterate a cipher, iterate it a prime number of times.
- This is all easily derived from analytic combinatorics, the study of exponential and ordinary generating series.
- Buy my book “Algebraic Cryptanalysis”, published by Springer, available now on Amazon.com.