

# Bezpieczeństwo systemów komputerowych

Jak silny jest szyfr?

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

23 października 2010

Na podstawie:

Bruce Schneier, Crypto-Gram Newsletter, 15 sierpnia 2009,

<http://www.schneier.com/crypto-gram-0908.html>

## Co jakiś czas pojawiają się artykuły informujące o złamaniu jakiegoś szyfru

- [1] A. Biryukov, D. Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256,  
<http://eprint.iacr.org/2009/317>
- [2] A. Biryukov, D. Khovratovich, I. Nikolić, Distinguisher and Related-Key Attack on the Full AES-256 (Extended Version),  
<http://eprint.iacr.org/2009/241>
- [3] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds,  
<http://eprint.iacr.org/2009/374>

# Co umiano poprzednio?

- ▶ Najlepsze poprzednio znane, ale niepraktyczne ataki wymagają:
  - ▶  $2^{128}$  operacji dla AES-128 (wyczerpujące przeszukiwanie),
  - ▶  $2^{176}$  operacji dla AES-192,
  - ▶  $2^{119}$  operacji dla AES-256.

## Co pokazano w [3]?

- ▶ 9-rundowy AES-256 można złamać:
  - ▶ wykonując  $2^{39}$  operacji,
  - ▶ wymaga dwóch zależnych kluczy.
- ▶ 10-rundowy AES-256 można złamać:
  - ▶ wykonując  $2^{45}$  operacji,
  - ▶ wymaga silniejszych zależności między podkluczami.
- ▶ 11-rundowy AES-256 można złamać:
  - ▶ wykonując  $2^{70}$  operacji.
- ▶ Przypomnijmy, że w rzeczywistości:
  - ▶ AES-128 wykonuje 10 rund,
  - ▶ AES-192 wykonuje 12 rund,
  - ▶ AES-256 wykonuje 14 rund.

## Dlaczego nie ma powodu do paniki?

- ▶ Atak korzysta ze słabości rozdziału klucza w AES-256.
- ▶ Atak nie przenosi się na AES-128.
- ▶ Atak korzysta z zależności między kluczami (ang. related-key attack), co wymaga poznania szyfrogramów tego samego tekstu jawnego zaszyfrowanego za pomocą wielu kluczy zależnych od siebie w specyficzny sposób.
- ▶ Atak dotyczy tylko 11-rundowego AES-256.

# Margines bezpieczeństwa

- ▶ Jeśli można złamać szyfr  $n$ -rundowy, zaprojektuj szyfr  $2n$  lub  $3n$ -rundowy.
- ▶ Margines bezpieczeństwa AES-a jest mniejszy niż dotychczas przypuszczano.
- ▶ Schneier sugeruje:
  - ▶ rozszerzenie AES-128 do 16, AES-192 do 20, a AES-256 do 28 rund,
  - ▶ nieużywanie AES-256 w nowych aplikacjach.
- ▶ Nie ma powodu do rezygnowania z AES-256 w istniejących aplikacjach.
- ▶ AES-128 nadal zapewnia dostateczny margines bezpieczeństwa w dającej się przewidzieć przyszłości.