Kryptografia, Lista 2

Adrian Mucha, Politechnika Wrocławska, WPPT 17/05/2020

AES vs. DES

AES	DES
AES: Advanced Encryption Standard	DES: Data Encryption Standard
Klucze mają długość 128, 192 lub 256 bitów	Długość klucza to 56 bitów.
Liczba rund w zależności od klucza: 10(128-bitów), 12(192-bitów) lub 14(256-bitów)	16 rund identycznych operacji
Struktura opiera się o sieć substytucyjno-permutacyjną.	Struktura opiera się o sieci Feistela.
AES jest bezpieczniejszy niż DES i jest światowym standardem.	DES może być łatwo złamany i ma wiele znanych słabości. Istnieje 3DES który jest bezpieczniejszy niż DES.
Koduje 128 bitów tekstu jawnego.	Koduje 64 bity tekstu jawnego.
Brak znanych ataków crypto-analitycznych prócz ataków side channel.	Znane ataki: Brute-force, Linear crypt-analysis oraz Differential crypt-analysis.

Tryby AES

AES obsługuje różne tryby operowania na danych, które posiadają różne właściwości i stopnie bezpieczeństwa oraz szybkości działania czy możliwości pracy równoległej na wielu blokach.

Tryb	Zalety	Wady
ECB	• Prosty • Szybki • Równoległy	• Powtórzenia tekstu jawnego będą widoczne w szyfrze • Uszkodzony szyfr będzie mieć wpływ na tekst jawny • Brak odporności na *replay attacks* • Nie powinno się go używać
CBC	• Równoległe odszyfrowywanie • Powtórzenia nie będą widoczne w szyfrze	• Brak równoległego szyfrowania • Uszkodzony blok wpływa na kolejne bloki
CFB	• Brak wyrównania (no padding) • Równoległe odszyfrowywanie	• Brak równoległego szyfrowania • Brak odporności na *replay attack* • Uszkodzony blok wpływa na kolejne bloki
OFB	• Brak wyrównania (no padding) • Szyfrowanie i deszyfrowanie używa tego samego schematu • Uszkodzony blok nie wpływa na inne	• Brak równoległego szyfrowania • Adwersarz może zmienić uszkodzić część szyfru by zmienić tekst jawny
CTR	• Brak wyrównania (no padding) • Równoległe szyfrowanie i deszyfrowanie • Szyfrowanie i deszyfrowanie używa tego samego schematu • Uszkodzony blok nie wpływa na inne	• Adwersarz może zmienić uszkodzić część szyfru by zmienić tekst jawny