Chaos-Based Symmetric Key Cryptosystems

Christopher A. Wood
Department of Computer Science
Rochester Institute of Technology, Rochester, New York, USA
caw4567@rit.edu

July 22, 2011

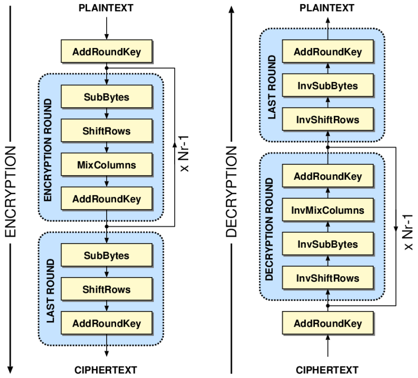
Outline

History of symmetric key ciphers

- Data Encryption Standard (DES) selected as an official FIPS standard in 1976
  - Brute force attacks require a 2^{56} steps - now feasible
  - Linear cryptanalysis revealed weaknesses in the design that could reduce the time complexity of a successful attack to $2^{29.2}$
  - Several replacement ciphers were proposed, including 3DES, Blowfish, RC5, and IDEA
- Advanced Encryption Standard (AES) competition held to replace the aging DES cipher
  - 1997 to 2001 - competition with 15 different symmetric key design proposals, including Rijndael, Serpent, Twofish, RC6, and MARS

AES (Rijndael)

- Round-based symmetric key cipher for blocks of 128 bits
- Key sizes of 128, 192, and 256 bits
  - Brute force attacks infeasible given current computing limitations
- Operates on elements in $GF(2^8)$ defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$

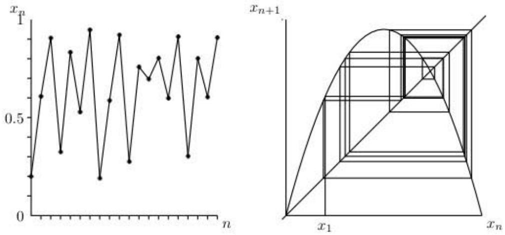


Chaos dynamics

Chaotic systems are characterized by the following properties:

1. Sensitivity to initial conditions
2. Dense collection of points with periodic orbits
3. Topologically mixing

Logistic map



$$x_{n+1} = rx_n(1 - (x_n)) \ (x_n, r \in \mathbb{R})$$

- Discrete time-based recurrence relation derived from the differential logistic equation
- r and x_0 are the initial conditions of the system

Mapping chaos theory to cryptography

Chaos theory	**Cryptography**
Mixing	Diffusion
Iterations	Rounds
Initial conditions	Keys
Continuous phase space	Finite phase space

A quick example - the Simple Cipher

- Design concepts
  - Based on the logistic map for its non-linear transformation
  - Uses the secret key to generate initial conditions for the map
  - Translates elements from the set of keys (2^8) to elements in $(0, 1]$ for the map
- Naïve approach
  - Does not follow traditional block cipher structure (think multi-stage encryption in AES)
  - Uses "real" numbers in the logistic map - expensive FLOPS lead to poor performance
  - Periodic behavior induced by system reliance on keys alone - leads to information leakage

Chaos-based cipher design

- Chaotic maps are non-linear transformations
  - Can be used to replace other non-linear transformation steps in the cipher (e.g. S-box substitution)
- Chaotic maps are topologically mixing
  - Add diffusion to mixing transformations in the cipher (e.g. MixColumns in AES)
- Chaotic maps are sensitive to initial conditions
  - Can be exploited to provide pseudorandomness to cipher operations (e.g. key generation, non-linear confusion routines)

Limitations

- No formal definition for discrete chaos in finite domains
- Chaotic behavior is approximated using one or more non-linear maps in space-discretized (finite) domains
- Proper security analysis often includes Hamming and Euclidean distance measures for chaotic maps

Cipher evaluation

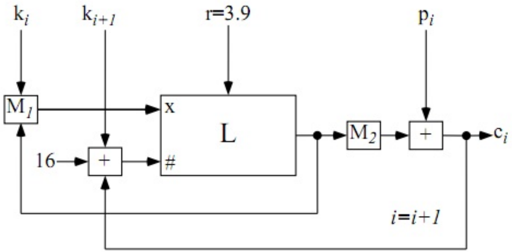
- **Theoretical** - ciphers possess "randomness increasing" and "computationally unpredictable" characteristics
- **Practical** - ciphers are resistant to known attacks
  - Ciphers should also be strong against trajectory-based, loss of information, and memory attacks
- An analysis of the entropy of a cipher is a good indication of its pseudorandom properties
- Statistical tests can be conducted to determine a PDF for elements of a trajectory

Case studies

- Advanced Cipher [K. Roskin and J. Casper]
- Rabbit Cipher [M. Boesgaard et al., 2003]
- Chaotic Feistel Cipher (not included in this talk) [L. Kocarev et al., 2006]

Advanced Cipher

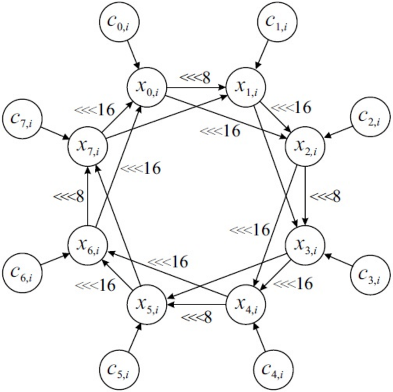
- Enhancement to the Simple Cipher
- Provides a feedback element for increased pseudorandomness and diminished periodic behavior
- Was shown that a single bit change in the encryption key effected approximately 49.6% of the ciphertext bits



Rabbit

- Approximates chaos with a system of eight coupled non-linear maps

  $x_{j,i}$ (next state variable)
  $c_{j,i}$ (counter)



Rabbit

- Some key design aspects
  - The next state function and counter dynamics are based on systems of non-linear maps
  - Phase space of 2^{32} elements
  - Does not rely on real number approximations - only uses integers
- Analysis
  - Hamming distance analysis revealed high levels of entropy for the chaotic map
  - Periodic behavior and algebraic analysis efforts were also done
    - Approached the analysis from a cryptographic perspective and dynamical systems perspective

Conclusion

Chaos-based symmetric key ciphers struggle for success:

- Lack of definition for discrete chaos in finite domains
- Inefficiencies of current implementations (typically related to FLOPS and real number representations)
- Thorough security analysis is difficult and often times indicates that practical chaos-based ciphers are inferior in security to standardized ciphers