

(1)

CHAOS BASED CRYPTOGRAPHY : A NEW APPROACH TO SECURE COMMUNICATIONS.

BARC NEWSLETTER

No. 258 July 2005

D.V. Lawande Theoretical Physics Division.

B.R. Ivan and S.D. Dhadapkar Reactor Control Division.

Cryptography : is the science of protecting the primary information during communication under hostile (opponents/hackers are present) conditions

- Current cryptographic techniques are based on Numer theoretic or Algebraic concepts, but Chaos is on another paradigm (type).
- Chaos is an offshoot of non-linear dynamics and was studied widely.
- Chaotic behaviour is a subtle behaviour of a non-linear system, which apparently looks random.
 - However, this randomness is not stochastic origin (not probability)
 - Randomness arises from the system's deterministic nature, where future states are fully determined by initial conditions
 - The key characteristics of chaos is its extreme sensitivity to these initial conditions, meaning even tiny, unmeasurable differences in the starting point can lead to vastly different outcomes.

creating the illusion of randomness

(2)

chaotic dynamics properties

- The discovery of chaotic synchronization principles by Pecora & Carroll became main cause to realisation of secure communications using chaotic behaviour in early 1990's.

i) Ergodicity : a system's trajectory, starting from almost any initial condition, will eventually explore all parts of its accessible state space, making time averages and ensemble averages equivalent.

→ In an ergodic system, the time averages of a quantity (calculated over a long time for a single trajectory) will be equal to the ensemble average (calculated by averaging over many different initial conditions at a single time).

ii) Sensitivity ("butterfly effect") : The tiny to smaller, even a tiny unmeasurable change can be the outcome of results in a very different outcome.

NOTE : The system is highly sensitive, a tiny change can occur a very different outcome but the change comes same (bcz of ergodicity).

chaotic behaviour simulation

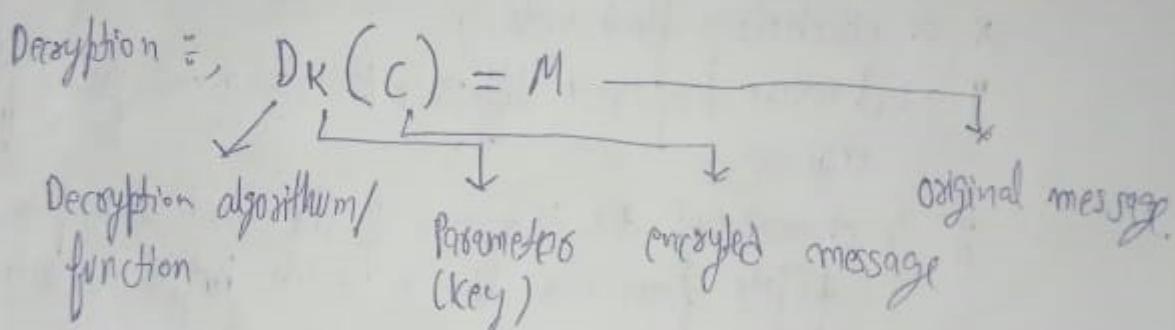
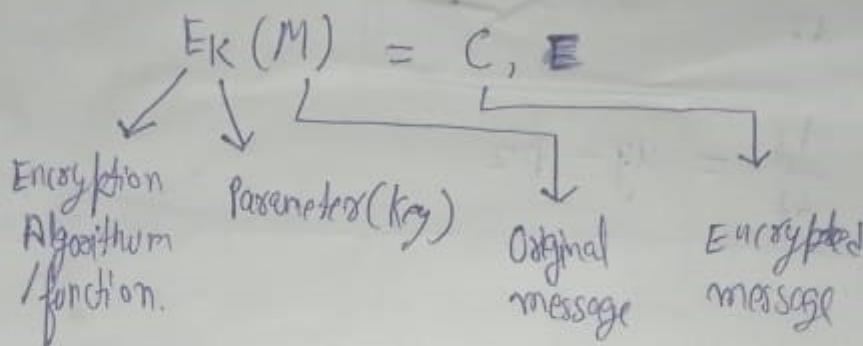
can be done using 3 or more discrete maps or in higher dimensional physical system described by 3 or more first order autonomous differential equations etc.

3

Cryptographic Definitions (Most basic.)

Plain M : Plaintext [a stream of bits, a text file, a bitmap, etc. (message)]

Encryption process of disguising a message M so as to hide its contents



NOTE: keys are known to sender and receiver.

key space: The set of permissible values that keys can take is called a key space.

Symmetric keys.

If sender and receiver uses same key.

$$E_K(M) = C$$

$$D_K(C) = M$$

Asymmetric keys

if the sender and receiver uses different keys.

$$E_{K_1}(M) = C$$

$$D_{K_2}(C) = M$$

Lorenz system : Atmospheric scientist E Lorenz proposed this system (1963) as a set of 3 ordinary differential equations to model a thermally induced convection in the atmosphere.

$$\frac{dx}{dt} = \sigma(y - x), \quad \frac{dy}{dt} = Rx - y - xz,$$

$$\frac{dz}{dt} = xy - bz$$

where,

x : circulatory fluid velocity

y : characterise temperature difference b/w rising and falling fluid regions.

z : characterized the distortion of the vertical temperature profile from its linear with height variation.

σ : related to Prandtl number

R : related to Rayleigh number

B : is a geometric factor.

(5)

* Chaos and Cryptography

- Cryptographic main strength lies in between the selection of keys (which are secret parameters and should not be guessed by an intruder).
- Chaotic ~~key~~ encryption can be obtained if we use parameters as keys, trajectories as encryption / decryption function.
- Chaotic scheme is symmetric. The parameters and the initial conditions form a very large key space thereby enhancing the security of code.

* Baptista Method & Logistic Map.

• used logistic map

• equation,

$$x_{n+1} = \gamma x_n (1 - x_n)$$

↓ ↓
Value in Value from previous iteration
current iteration. Parameters

- initial condition, $x_0 \in [0, 1]$
- A set of large number of these it rates [$\approx 60,000$] is called trajectory.
- and each value are lies in $(0, 1)$.

⑥

Trajectory mapping

Now one can very easily figure out using the cipher text but he is unaware of X_{\min}, X_{\max} so he don't know the range of matching point from where?

An interval $[X_{\min}, X_{\max}]$ of the trajectory generated in step (1) is divided into $S \leq 256$ sites (cells) each of size $\epsilon = \frac{X_{\max} - X_{\min}}{S}$. To each of these sites, a byte or an ASCII character is associated as typically shown below.

X_{\min}	?	A	b	.	.	\$	#	@	*	X_{\max}
1	a	3	4	o	o	5-3	5-2	5-1	5	

• for encryption, each character of a text, one finds the number of iterations necessary to reach the required site belonging to that character. The number of iterations is the cipher text of the character.

The process is repeated till the whole message is encrypted into a set of numbers. This forms the cipher text.

(7)

Decryption is done by running the same algorithm with the same keys and the number of iterations equal to the integer values in the cipher text and by reverse mapping the site numbers into the characters.

Note: A Encryption project is made by Nitash (Based on Baptista's method or Baptista's Equation)

★ Chaos Based on Lorenz dynamics.
The Lorenz system is a set of three non-linear differential equations developed by Edward Lorenz in 1963 to model atmospheric convections.

$$\left\{ \begin{array}{l} \frac{dx}{dt} = \sigma(y - x) \\ \frac{dy}{dt} = x(\rho - z) - y \\ \frac{dz}{dt} = xy - bz \end{array} \right.$$

where:
 σ is the conversion rate
 y is the temperature difference
 z is the vertical temperature difference
 σ, ρ, b are system parameters (positive constants).

Typical values,

$$\sigma = 10 \quad \rho = 28$$

$$b = 8/3$$

Trajectory folding (Modulo mapping)

To create a bounded, dense distribution, the system variable are folded using

$$x' = x \bmod p, \quad y' = y \bmod p$$

$$z = z \bmod p$$

- The parameter p is typically in range $[1, 5]$, and acts as an additional encryption key.
- This creates dense and uniformly distributed values, useful for mapping to characters.

Variable selection and cell partitioning

- run the Lorenz system at least 60000 points
- choose one variable $v \in \{x, y, z\}$ (say x) for encryption
- from the density plot (like histogram), select a range $[v_{\min}, v_{\max}]$ with fairly uniform frequency (≈ 100).
- Divide this range into $S \leq 256$ cells.

$$\epsilon = \frac{v_{\max} - v_{\min}}{S}$$

each cell is assigned a unique ASCII character (0-255)

(7)

A ~~Encryption~~ ~~minitaur~~, i have made using Baptista's method.

encryption using Baptista-style scheme

let say $M = \text{"Hello"}$

For each character

1. Run Lorenz dynamics with initial conditions $x(0)$ and $y(0)$ and $z(0)$ and parameters σ, β, ρ
 2. Transform the chosen values variables, $v = x \bmod p$
 $(\text{or } v = y \bmod p, v = z \bmod p)$
 3. Iterate through the trajectory until v lands in the cell corresponding to the target character.
 4. Count how many iterations (time steps) it took → that's your cipher number n .
 5. Optionally, add randomness using: ~~#this~~
 (Note: this is useful to save from pattern attacks
 bcz it generates different ciphers for same msg
 with same parameters)
 - random number $k \in [0, 1]$
 - threshold $n \in [0, 1]$ if $k > n$, accept n .
- repeat for each character.

The ciphertext becomes list of integers

Cn [1100, 3547
2412 etc]

4. Decryption

To decrypt

- Use the same initial conditions and parameters
- for each $n_i \in C_m$ run the system for n_i steps
- Find the cell in which the variable ϑ lies.
- Map the cell index to its ASCII character.

Security considerations

- The chaotic system of logic system ensures unpredictability
- The key includes:
 - Initial condition : $x(0), y(0), z(0)$
 - Parameters : σ, β, ρ
 - Folding parameter : P
 - Selected variable : ϑ
 - Range : v_{\min}, v_{\max}
 - Mapping function
 - Random threshold n
 - Transient Number N_0 .

This makes key space large and difficult to brute-force.

Conclusions

- ⇒ To be protected from pattern attacks we can do
apply side - mesh randomisation or by "superimposing"
a random text on the original text.
- ⇒ Babbistek's scheme gives chain encryption, which has
the disadvantage of making the rest of the
ciphertext erroneous even if a single character
is corrupted during communications.

Nilash Varma