Dynamics at the Horsetooth Volume 2, 2010.

Security from Chaos

Francis Motta
Department of Mathematics
Colorado State University motta@math.colostate.edu

Report submitted to Prof. P. Shipman for Math 540, Fall 2010

Abstract. A degree-three polynomial with a single parameter is constructed and its connection, as a discrete dynamical system, to the shift map on three indices is explored. For each $2 \leq n \in \mathbb{N}$ a piecewise continuous function on $[0, 1]$ with a single parameter is constructed and a topological conjugacy is demonstrated between the shift map on n symbols and this function. Using the correspondance for $n = 10$ a theoretical algorithm is developed to construct dynamic passwords which depend on time. The chaotic nature of the shift map and its sensititvity to initial conditions suggests a robust and difficult to break dynamic password system.

1 Introduction

It is shown in [1] that the logistic map $x_{n+1} = f(x_n) = \lambda x_n(1 - x_n)$ is topologically conjugate to a dynamical system which is much more easy to understand (when $\lambda > 4$). That dynamical system is the shift map on on the set of all binary sequences. Properties of the dynamics such as sensitivity to initial conditions and the existence of dense orbits are more easily seen in the shift map and so the conjugacy allows us to easily prove that the logistic map exhibits chaotic behavior for certain values of its parameter. In Section 2 we rigorously define the shift map on the set of all sequences over $\{0, 1, 2, ..., n\}$ and demonstrate some of the characterisitics of the map and this set. In Section 3, we use the characteristics of the logistic map to extend to a degree-three polynomial which can be shown to be conjugate to the shift map on three indices, and we generalize this completely with the construction of a family of piecewise linear maps. We then use this result to construct a method of dynamically generating passwords. The goal of such a system is combat keyloggers which can be installed on one's computer without their knowledge with the intention of stealing their passwords. Passwords which remain valid only for a short period of time negate most of the effectiveness of keyloggers.

2 The Shift Map

Definition 2.1 For $2 \leq n \in \mathbb{N}$ let $\Sigma_n = \{\phi : \mathbb{Z}^+ \to \{0, 1, 2, ..., n - 1\}\} = \{(a_i) : a_i \in \{0, 1, 2, ..., n - 1\} \text{ for each } i \in \mathbb{Z}^+\}$. That is to say Σ_n is the set of all sequences over the set of nonnegative integers less than n. For example Σ_2 is the set of all binary sequences and Σ_3 is the set of all ternary sequences.

Definition 2.2 Let $d : \Sigma_n \times \Sigma_n \to \mathbb{R}$ be defined as follows:

$$d((a_i), (b_i)) = \sum_{i=0}^{\infty} \frac{|a_i - b_i|}{2^i}$$

Proposition 2.3 d is a metric on Σ_n

Proof:

That d is well defined requires convergence of the series for any $(a_i), (b_i) \in \Sigma_n$. Observe that $|a_i - b_i| \leq n-1$. Thus $d((a_i),(b_i)) \leq \sum_{i=0}^{\infty} \frac{n-1}{2^i} = (n-1)\sum_{i=0}^{\infty} \frac{1}{2^i} = 2(n-1) < \infty$.

Also that d is a metric is easily verified. Let $(a_i), (b_i), (c_i) \in \Sigma_n$.

$d((a_i),(a_i)) = \sum_{i=0}^{\infty} \frac{|a_i - a_i|}{2^i} = \sum_{i=0}^{\infty} \frac{0}{2^i} = 0$. Now assume $d((a_i),(b_i)) = 0$ then $a_i = b_i$ for each i since if not then $\frac{|a_j - b_j|}{2^j} > 0$ for some j, therefore $(a_i) = (b_i)$ and d satisfies the identity of indiscernibles.

$d((a_i),(b_i)) = \sum_{i=0}^{\infty} \frac{|a_i - b_i|}{2^i} = \sum_{i=0}^{\infty} \frac{|b_i - a_i|}{2^i} = d((b_i),(a_i))$. This shows d is symmetric.

$$d((a_i),(c_i)) = \sum_{i=0}^{\infty} \frac{|a_i - c_i|}{2^i}$$
$$= \sum_{i=0}^{\infty} \frac{|(a_i - b_i) + (b_i - c_i)|}{2^i}$$
$$\leq \sum_{i=0}^{\infty} \frac{|(a_i - b_i)| + (b_i - c_i)|}{2^i}$$
$$= \sum_{i=0}^{\infty} \frac{|a_i - b_i|}{2^i} + \sum_{i=0}^{\infty} \frac{|b_i - c_i|}{2^i}$$
$$= d((a_i),(b_i)) + d((b_i),(c_i)).$$

And thus d satisfies the triangle inequality. $\diamond$

Definition 2.4 For each n we can construct the following function $\sigma : \Sigma_n \to \Sigma_n$ by

$$\sigma((a_i)) = (a_{i+1})$$

In other words, if $(a_i) = (a_0, a_1, a_2, ...)$ then $\sigma((a_i)) = (a_1, a_2, a_3, ...)$.

In [1] it is shown that the logistic map is topologically conjugate to σ as a map on Σ_2 for certain parameter values. That is, the dynamics of the logisitics map are in a certain sense equivalent to the dynamics of the shift map. Since our goal is to generalize this to the shift map σ as a function on Σ_n and take advantage of those properties in the construction of a dynamic password algorithm, we make note of a few properties that must be considered to successfully construct such a continuous function.

Remark 2.5 σ is an n-to-one map since for any $(a_i) \in \Sigma_n$ we have $\sigma(s, a_0, a_1, a_2, ...) = (a_i)$, for each $s \in \{0, 1, 2, ..., n-1\}$. Therefore a strong symmetry must exist in any dynamical system $x_{n+1} = f(x_n)$ that is conjugate to the shift map since for every $x_0 \in \Lambda_n$ there must be exactly $n-1$ other initial conditions $\{y(1), ..., y(n-1)\}$ such that $f^k(x_0) = f^k(y(i))$ for every i, k.

Remark 2.6 It is obvious that σ has periodic orbits of every length. In fact there are exactly n^k periodic orbits of length k since for each $k \in \mathbb{Z}^+$ there are n^k different blocks of length k consisting of integers from $\{0, 1, 2, ..., n-1\}$. Repetition of such a block defines a point in Σ_n which is on a periodic orbit of length k and any sequence (a_i) with $\sigma^k((a_i)) = (a_i)$ is a sequence consisting of repeated blocks of length k. Thus any conjugate dynamical system $x_{n+1} = f(x_n)$ will necessarily have the property that $f^k(x) - x = 0$ will have exactly n^k real solutions ($k \geq 1$) corresponding to points on periodic orbits of length k of f.

With these ideas in mind, we propose a degree-three polynomial with a single parameter defined on $[0,1]$ which could be shown to be topologically conjugate to $\sigma : \Sigma_3 \to \Sigma_3$ and investigate some of its properties numerically. Then, for each $n \geq 2$ we define a piecewise-linear, continuous function and demonstrate that it is topologically conjugate to $\sigma : \Sigma_n \to \Sigma_n$.

3 Generalizations of the Logistic Map

Remarks 2.5 and 2.6 as well as an understanding of invariant set Λ associated with the logistic map naturally lead us to consider a degree three polynomial with parameter $\epsilon \in \mathbb{R}$:

Definition 3.1

$$p : [0,1] \to [-\epsilon, 1+\epsilon]$$
$$p(x) = a_3x^3 + a_2x^2 + a_1x$$

subject to the following constraints:

$$p(0) = 0$$
$$p(1) = 1$$
$$p(1/2) = 1/2$$
$$p(1/4) = 1+\epsilon$$
$$p(3/4) = -\epsilon$$

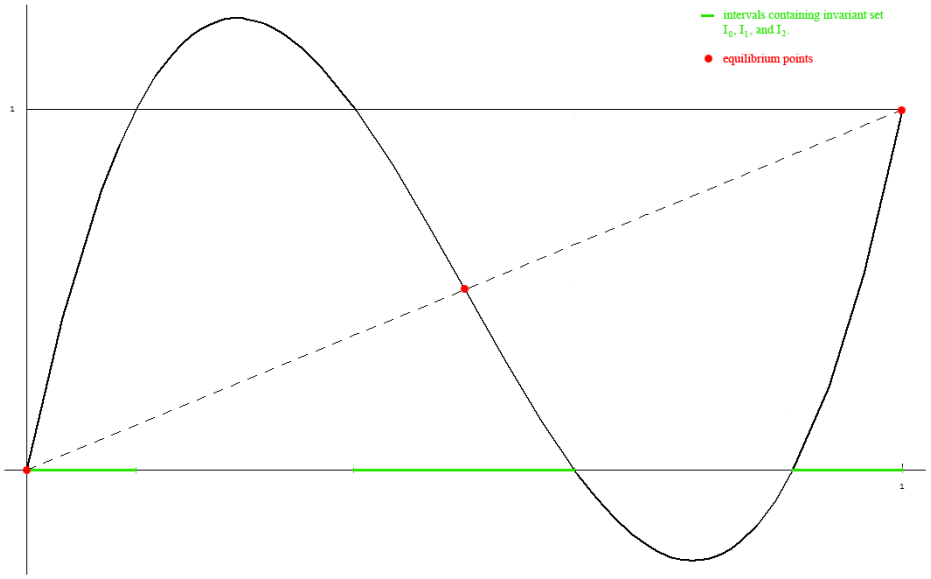


Figure 1: prototypical example of p(x)

These conditions allow us to solve for the coefficients a_1, a_2, a_3:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1/2 & 1/4 & 1/8 \\ 1/4 & 1/6 & 1/64 \\ 3/4 & 9/16 & 27/64 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1/2 \\ 1+\epsilon \\ -\epsilon \end{pmatrix}$$

$$\implies a_3 = \tfrac{64}{3}\epsilon + 16, a_2 = -(32\epsilon + 24), a_1 = \tfrac{32}{3}\epsilon + 9$$

$$\implies p(x) = (\tfrac{64}{3}\epsilon + 16)x^3 - (32\epsilon + 24)x^2 + (\tfrac{32}{3}\epsilon + 9)x$$

As with the logistic map $x_{n+1} = f(x_n) = \lambda x_n(1 - x_n)$ (when $\lambda > 4$) the map $x_{n+1} = p(x_n)$ (with $\epsilon > 0$) has a range which is a proper superset of $[0, 1]$, its domain. In other words, there exist open intervals $A_0, A_1 \subset [0, 1]$ with the property that for any $x \in A_0, p(x) > 1$ and for any $x \in A_1, p(x) < 0$. We can solve for these intervals explicitly in terms of ϵ and, similarly, define the closed intervals which are invariant under a single iteration of p.

$$A_0 = \left[\tfrac{4\epsilon-2\sqrt{\epsilon(4\epsilon+3)}+3}{16\epsilon+12}, \tfrac{4\epsilon+2\sqrt{\epsilon(4\epsilon+3)}+3}{16\epsilon+12}\right]$$
$$A_1 = \left[\tfrac{12\epsilon-2\sqrt{\epsilon(4\epsilon+3)}+9}{16\epsilon+12}, \tfrac{12\epsilon+2\sqrt{\epsilon(4\epsilon+3)}+9}{16\epsilon+12}\right]$$
$$I_0 = \left[0, \tfrac{4\epsilon-2\sqrt{\epsilon(4\epsilon+3)}+3}{16\epsilon+12}\right]$$
$$I_1 = \left[\tfrac{4\epsilon+2\sqrt{\epsilon(4\epsilon+3)}+3}{16\epsilon+12}, \tfrac{12\epsilon-2\sqrt{\epsilon(4\epsilon+3)}+9}{16\epsilon+12}\right]$$
$$I_2 = \left[\tfrac{12\epsilon+2\sqrt{\epsilon(4\epsilon+3)}+9}{16\epsilon+12}, 1\right]$$

Remark Rather than go through the complete construction of the invariant set we simply remark on the existence of a Cantor-like set of points we would call Λ_3 with the property that $x_0 \in \Lambda_3 \implies x_k = p^k(x_0) \in \Lambda_3$ for all $k \in \mathbb{Z}^+$. This set is the complement in $[0, 1]$ of the union over all $i \in \mathbb{Z}^+$ of the intervals A_0^i and A_1^i defined by $x \in A_j^i$ if $p^i(x) \in A_j$ (i.e. those points which eventually leave the interval [0,1] after sufficiently many iterations of p).

As before, the itinerary of a point $x_0 \in \Lambda_3$ is given by the map $S : \Lambda_3 \to \Sigma_3$ defined by $S(x_0) = (a_0, a_1, a_2, ...)$ where $a_j = k$ iff $p^j(x_0) \in I_k$.

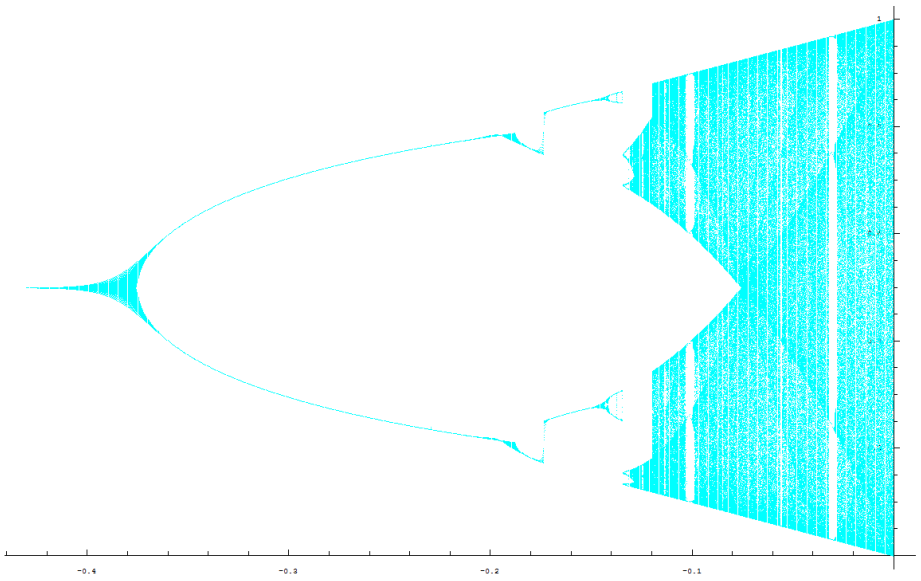
As stated, it can be shown following the proof in [1] that for $\epsilon > \frac{3}{32}(3\sqrt{2} - 4) \approx 0.0227476$, S is a homeomorphism. It is conjectured that S is a homeomorphism for $\epsilon > 0$ but a simple proof which we will give later for the more general dynamical system relies on the absolute value of the derivative of p being larger than 1 on I_0, I_1, and I_2 which is only true for $\epsilon > \frac{3}{32}(3\sqrt{2} - 4)$.

Rather than prove the conjugacy explicitly for this case we investigate the remarks in the previous section. By construction the points $x_0 = 0, y_0 = 1/2$ and $z_0 = 1$ are fixed by p and are identified by the map S with the sequences $(\bar{0}) = (0, 0, 0, ...), (\bar{1}) = (1, 1, 1, ...)$, and $(\bar{2}) = (2, 2, 2, ...)$. But if S is indeed a bijection there must exist nine initial conditions in $[0, 1]$ each corresponding to one of the 2-cycles easily observed in Σ_3 (i.e. $(\bar{01}), (\bar{02}), (\bar{12})$, etc.) Clearly $x_0 = 0, y_0 = 1/2$ and $z_0 = 1$ are three of these nine points which are on cycles of length 2 and using numerical methods we are able to approximate the other six.

To do so,we fix $\epsilon = .025$ and solve $p(p(x)) - x = 0$.

x	x $\in I_k$	p(x)	p(x) $\in I_k$	S(x)
0	I_0	0	I_0	$(\bar{0})$
0.0904858675726023	I_0	0.6476966633832572	I_1	$(\bar{01})$
0.1407893959464495	I_0	0.8592106040523758	I_2	$(\bar{02})$
0.3523033366169359	I_1	0.9095141324288261	I_2	$(\bar{12})$
1/2	I_1	1/2	I_1	$(\bar{1})$
0.6476966633832572	I_1	0.0904858675726023	I_0	$(\bar{10})$
0.8592106040523758	I_2	0.1407893959464495	I_0	$(\bar{20})$
0.9095141324288261	I_2	0.3523033366169359	I_1	$(\bar{21})$
1	I_2	1	I_2	$(\bar{2})$

Using numerical approximations of the equilibrium points and limit cycles the following bifurcation diagram was constructed for the map $x_{n+1} = p(x_n)$ as the parameter ϵ was allowed to vary using a publically available mathematica program [2].



The above construction shows how one might go about building a degree n-polynomial discrete-time-dynamical-system with a single parameter that is topologically conjugate to the shift map on Σ_n. However for simplicity, explicitness and to demonstrate the fact that the above construction is only one possible method of building a dynamical system defined on the interval $[0,1]$ which is conjugate to the shift map on n-symbols we now define a class of piecewise linear functions on the unit interval.

Definition 3.2 Fix $n \in \mathbb{Z}^+, n \geq 2$ and $\epsilon > 0$.

Define a partition of $[0,1]$ by $x_1 = 0$, $x_{n+1} = 1$, and $x_i = \frac{i(1+2\epsilon)-(3\epsilon+1)}{2\epsilon(n-1)+n}$ for $i = 2, 3, ..., n$.

Definition 3.3

If n is even:

$$p_n(x) := \begin{cases} (2\epsilon(n-1)+n)x & \mathrm{x}_1 = 0 \leq x \leq x_2 \\ \text{-}(2\epsilon(n-1)+n)(x-x_i)+(1+\epsilon) & \mathrm{x}_i \leq x \leq x_{i+1}, i\text{-even} \\ (2\epsilon(n-1)+n)(x-x_i)-\epsilon & \mathrm{x}_i \leq x \leq x_{i+1}, i\text{-odd} \\ \text{-}(2\epsilon(n-1)+n)(x-1) & \mathrm{x}_n \leq x \leq x_{n+1} = 1 \end{cases}$$

If n is odd:

$$p_n(x) := \begin{cases} (2\epsilon(n-1)+n)x & \mathrm{x}_1 = 0 \leq x \leq x_2 \\ \text{-}(2\epsilon(n-1)+n)(x-x_i)+(1+\epsilon) & \mathrm{x}_i \leq x \leq x_{i+1}, i\text{-even} \\ (2\epsilon(n-1)+n)(x-x_i)-\epsilon & \mathrm{x}_i \leq x \leq x_{i+1}, i\text{-odd} \\ \text{-}(2\epsilon(n-1)+n)(x-1)+1 & \mathrm{x}_n \leq x \leq x_{n+1} = 1 \end{cases}$$

We now discuss some of the easily verifiable properties of p_n.

p_n is continuous at all $x \in [0,1]$ and it can be seen in the definition that on each interval $[x_i, x_i+1], p_n$ is a linear function with slope $\pm 2\epsilon(n-1)+n$. For n-even, $p_n(0) = 0, p_n(1) = 0$ and for n-odd, $p_n(0) = 0, p_n(1) = 1$. p_n maps the unit interval onto the interval $[-\epsilon, 1+\epsilon]$.

As a dynamical system $x_{k+1} = p_n(x_k)$ there are fixed points at $x = \frac{2\epsilon(i-1)+i}{2\epsilon(n-1)+n+1}$ for $i = 2, 4, 6, ... < n$ and $x = \frac{i-1}{n-1}$ for $i = 3, 5, 7, ... < n$. These are unstable as $|p_n'(x)| = 2\epsilon(n-1) + n \geq 2 > 1$ since $n \geq 2$ and $\epsilon > 0$.

Definition 3.4 $H_i = \left[\frac{(2\epsilon+1)(i-1)}{2\epsilon(n-1)+n}, \frac{2\epsilon(i-1)+i}{2\epsilon(n-1)+n}\right], i = 1, 2, ..., n$

Definition 3.5 $B_i^0 = \left(\frac{2\epsilon(i-1)+i}{2\epsilon(n-1)+n}, \frac{(2\epsilon+1)i}{2\epsilon(n-1)+n}\right), i = 1, 2, ..., n-1$

Definition 3.6 $B_i^k = \{x \in [0,1] | p_n^k(x) \in B_i^0 \text{ for some } i\}$

Definition 3.7 $\Lambda_n = [0,1] - \bigcup_{k=0}^{\infty} B_i^k \subseteq \bigcup_{i=1}^{n} H_i$

By definition, Λ_n is the invariant set of of p_n. Moreover $p_n^k(x) \in H_i$ for some i for all $k \in \mathbb{Z}^+$ and $x \in \Lambda_n$. So consider $x_0 \in \Lambda_n$ and define $S : \Lambda_n \to \Sigma_n$ as before:

Definition 3.8 $S(x_0) = (a_0, a_1, a_2, ...)$ with $a_i \in \{0, 1, 2, ..., n-1\}, \forall i$ by $s_i = k$ iff $p_n^i(x_0) \in H_k$. That is, assign the value $k \in \{0, 1, 2, ..., n-1\}$ to the ith term of the sequence (a_i) if the ith iteration of p_n (starting at x_0) is in H_k.

The figure below shows p_7 and some of the sets defined above.

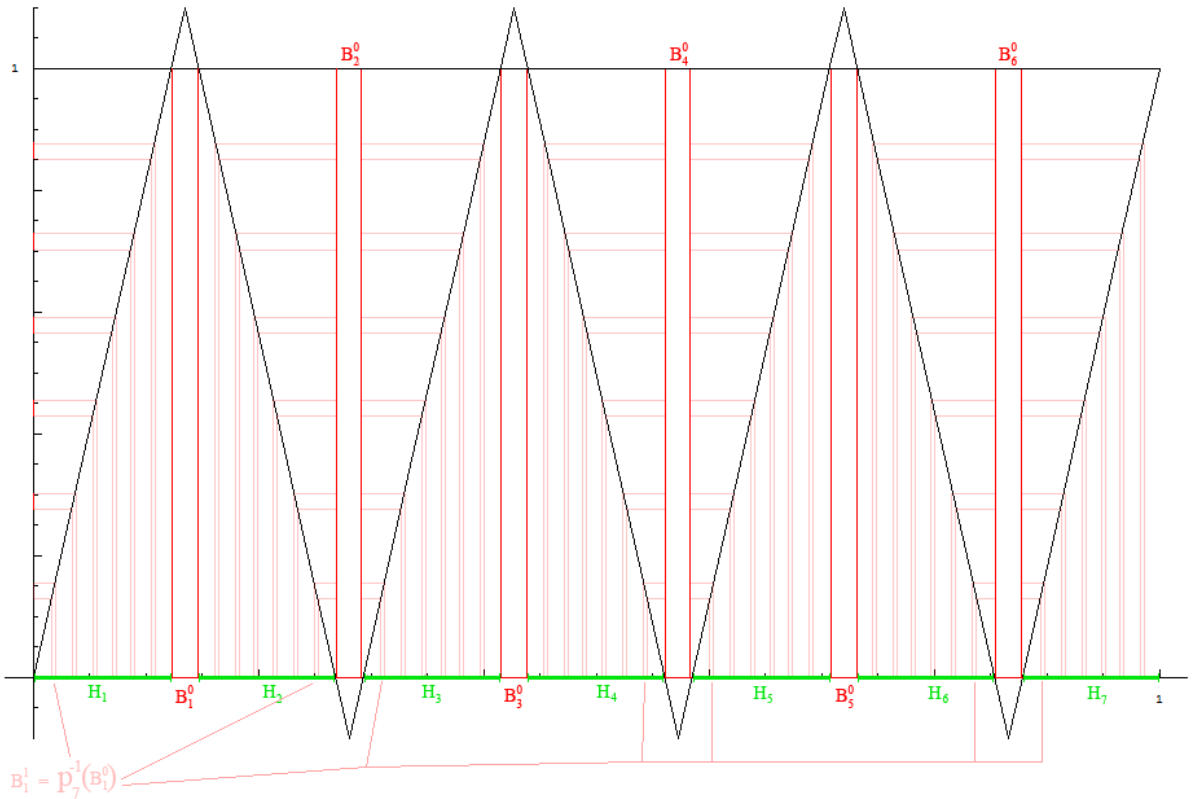


Figure 2:

Theorem 3.9 $S : \Lambda_n \to \Sigma_n$ is a bijection.

Proof:

Let $x \neq y \in \Lambda_n$ and assume $S(x) = (a_0, a_1, a_2, ...) = (b_0, b_1, b_2, ...) = S(y)$. Thus for each $k \in \mathbb{Z}^+$ $p_n^k(x)$ and $p_n^k(y)$ are both contained in H_{a_k}. Becuase p_n is monotone on the intervals H_i, the interval between $p_n^k(x)$ and $p_n^k(y)$, call it J_k, must also be contained in H_{a_k} for each k. But $p_n'(x) = 2\epsilon(n-1)+n \geq 2 > 1$ on J_k and therefore $|p_n^{k+1}(x) - p_n^{k+1}(y)| = (2\epsilon(n-1)+n)|p_n^k(x) - p_n^k(y)|$. In other words, the width of the intervals J_k grow without bound and therefore there exists m so large that $p_n^m(x) \in H_q$ but $p_n^m(y) \in H_p \neq H_q$ (for some q). Then $a_m = q \neq b_m = p$ which contradictions the assumption that $S(x) = S(y)$. Therefore $x = y$ which shows S is injective.

Now for any closed interval $J \subset [0,1]$ define $p_n^{-k}(J) = \{x \in [0,1] | p_n^k(x) \in J\}$. From Figure 2 it is clear that for any closed interval J, $p_n^{-1}(J)$ will consist of the union of n closed intervals, one in each H_i.

Let $(a_i) = (a_0, a_1, a_2, ...) \in \Sigma_n$ and for each $m \in \mathbb{Z}^+$ define $H_{a_0,a_1,...,a_m} = H_{a_0} \cap p_n^{-1}(H_{a_1}) \cap ... \cap p_n^{-m}(H_{a_m})$. Therefore

$$X := \bigcap_{i \geq 0}^{\infty} I_{a_0,a_1,...,a_i}$$

is nonempty as this is the intersection of nested closed intervals. So there exists some $x \in X$. By construction $x \in H_{a_0}$, $p_n(x) \in H_{a_1}$ and in general $p_n^k(x) \in H_{a_k}$. But this is exactly how we defined S and so $S(x) = (a_0, a_1, a_2, ...)$. We have shown that for any sequence $(a_i) \in \Sigma_n$ there exists a point $x \in \Lambda_n$ with $S(x) = (a_i)$ and thus S is surjective. $\diamond$

Knowing that S is a bijection will be enough to allow for the construction of a well-defined dynamic password system to be developed in the following section. However we will need to know more to analyse the security of such a system and, in fact, the proof of the following theorem will give insight into how to construct the algorithm for the dynamic password system.

We observed that Σ_n is a metric space in Section 2 where we defined the metric $d : \Sigma_n \times \Sigma_n \to \mathbb{R}$. Obviously Λ_n is a metric space with the usual Euclidean metric. The reason for introducing a metric on Σ_n was to prove that with respect to that metric the following theorem holds.

Theorem 3.10 $S : \Lambda_n \to \Sigma_n$ is continuous at each point $x \in \Lambda_n$.

Proof:

Let $x \in \Lambda_n$ with $S(x) = (a_0, a_1, a_2, ...)$ and let $e > 0$ be fixed. Pick $k \in \mathbb{Z}$ so large that $\frac{n-1}{2^k} < e$. Now consider $H_{a_0,a_1,...,a_k} = H_{a_0} \cap ... \cap p_n^{-k}(H_{a_k}) = [s,t]$ as defined in the previous theorem. This interval has width $\frac{1}{(2\epsilon(n-1)+n)^{k+1}}$ as an interval of length L will have preimage under p_n of length $\frac{L}{2\epsilon(n-1)+n}$. Define $\delta = \min s - x, x - t \leq \frac{1}{(4\epsilon(n-1)+n)^{k+1}}$. Then if $y \in \Lambda_n$ with $S(y) = (b_0, b_1, b_2, ...)$ and $|x - y| < \delta$ it follows that $y \in H_{a_0,a_1,...,a_k}$ as well and therefore $a_i = b_i$ for $i = 1, 2, 3, ...k$. Therefore $d(S(x), S(y)) = \sum_{i=0}^{\infty} \frac{|a_i - b_i|}{2^i} = \sum_{i=k+1}^{\infty} \frac{|a_i - b_i|}{2^i} \leq \frac{n-1}{2^k} < e$. $\diamond$

4 Dynamic Passwords

Consider the many online services which offer their customers access to their account via a webpage. Banks, email providers, online games, and many other businesses secure customer accounts with a username and password combination that is meant to prevent unauthorized access. But malicious software like keyloggers, which can be installed on a computer without the user's knowledge,

can monitor every keystroke thus making fixed username and password combinations useless at preventing unauthorized access. To combat this breech of security some systems offer or enforce the use of dynamic passwords that are valid only for a short period of time.

The general situation is as follows: A user wishes to access an account using a username and password combination. The username will remain fixed but the password will change at fixed time intervals according to some prescribed algorithm which is unique to the user and known only to the user and the account. Thus a password is valid only for a short time. If that time is very short, say less than 1 minute, the liklihood of a keylogger granting unauthorized access to the account is very low. In this, section we construct an algorithm for generating dynamic passwords based on the piecewise linear functions built in the previous section. Though we will not do a formal analysis of how secure these passwords are or discuss its potential vulnerabilities, we will discuss the system's sensitivity to initial conditions and the parameter value ϵ as indicators of robust security.

Definition 4.1 Let $U : \mathbb{N} \to (0, \infty) \times \mathbb{N} \times \mathbb{N}$ be an injective function that assigns to each natural number n a unique triple $U(n) = (\epsilon_n, T_n, P_n)$. T_n needs to be restricted to positive integers less than some upperbound (currently approximately 59,000,000; the number of minutes that have elapsed since 12:00am January 1st 1900) as it will be used as a zero point for the number of minutes that have elapsed for this user. For simplicity we will require that number to be positive. P_n captures the required level of precision to be used for this user. As we will, the passwords are unique numbers but in most cases irrational and will be approximated by a finite decimal expansion. The accuracy of this approximation need not be fixed for each user and is captured in P_n. So U can be thought of as the assignment of a unique seed to each account holder.

For the nth user assign to them $U(n) = (\epsilon_n, T_n, P_n)$. Now consider $p_{10} : \Lambda_{10,\epsilon_n} \subset [0, 1] \to \Lambda_{10,\epsilon_n} \subset [-\epsilon_n, 1 + \epsilon_n]$, the piecewise linear function built in Section 3 restricted to the invariant Cantor-like set, which was shown to be homeomorphic to the set of infinite sequences over $\{0, 1, 2, ..., 9\}$ (i.e. Σ_{10}) via the itinerary map $S : \Lambda_{10,\epsilon_n} \to \Sigma_{10}$. (Here we are just being explicit about the dependence of the invariant set on the parameter value ϵ_n).

Definition 4.2 If T is the current number of minutes that have elapsed since 00:00 January 1st, 1900 then $T - T_n$ is an integer and can be written as $a_k 10^k + a_{k-1} 10^{k-1} + ... + a_0$ for some k, where $a_i \in \{0, 1, 2, ..., 9\}$. Then $(a_i) := (a_0, a_1, ..., a_k, a_0, a_1, ..., a_k, ...) \in \Sigma_{10}$ and lies on a periodic orbit of the shift map of length k. Let $F : \mathbb{N} \to \Sigma_{10}$ be the injection that makes this association between integers and periodic sequences.

We have shown that there exists a unique $x \in \Lambda_{10,\epsilon_n}$ such that $S(x) = (a_i)$, where S maps x to its itinerary under iterations of p_{10} with parameter value ϵ_n.

Definition 4.3 Let $\Phi : \mathbb{N} \to \Lambda_{10,\epsilon_n}$ be the injective function $\Phi(T) = S^{-1}(F(T)) = x$. We say $\Phi(T)$ is the password valid for minute T.

Remark 4.4 For most sequences (a_i) the password can only be approximated in practice. For example we can easily build an interval of possible passwords which have itineraries that agree on the first n-terms of the associated sequence (the intervals between the B_i^k intervals constructed above). Also the real password for a given periodic sequences (as constructed by F) will be contained in these intervals. Thus the value of P_n represents how accurate the approximation of x is; in particular it represents the number of terms in the sequence associated with a point that must agree with the periodic sequence (a_i). In practice one might choose the left endpoint of the interval to represent the password. This will agree with the periodic sequence on the first P_n terms and then map to 0 on the P_nth iteration of p_{10}. Similarly you could pick the right endpoint which would agree with the periodic sequence on the first P_n terms and then map to 1 on the P_nth iteration of p_{10}.

Before we consider an example, we make a few observations.

Every minute will yield a password different from every minute before or after because of the bijective correspondance between Σ_{10} and Λ_{10}. The password is constructed deterministically. In other words, anyone with the same pair ϵ_n and T_n will have the same passwords for all time T. This is of course essential to the functioning of the system since both the user and the service must know the unique pair $U(n)$ assigned to the user in order to, respectively, produce and verify each password.

This system cannot completely prevent unauthorized access. Each password is valid for one minute and so a fast-acting keylogger could give a valid password to an unauthorized user. Furthermore, it might be possible through some clever attack, to determine a user's assignment (ϵ_n, T_n, P_n) given enough information. For example imagine a very effective keylogger watching a user log in hundreds of times. For each login the unauthorized user will know the current time T and the password generated by the user's unique seed (ϵ_n, T_n). Under what circumstances could they determine, or approximate well enough, one or both of these values? What is a good enough approximation? Answers to these questions depend on the particular algorithm used to approximate the password x (as we have said, x will generally be an irrational number expressed as an approximation in decimal expansion) and require further investigation to find.

Example 4.5 Consider the user n with seed assignment $\epsilon_n = .025$ and $T_n = 58, 115, 341$.

In the table below we construct several intervals which contain the correct password for login times minutes and days apart for $\epsilon_n = .025$. These intervals correspond to all points which agree with (a_i) for one period. In practice the exact password could not be determined precisely. Nonetheless this table demonstrates the effect of small changes in the initial condition and illustrates clearly that only dates/times corresponding to very similar sequences will yield similar passwords. Observe that such times are very far apart. For example (7,9,9,1,7,...) and (7,9,9,1,...) correspond for this user to logins nearly 3 months apart.

$$\epsilon_n = .025, T_n = 58, 115, 341, P_n = 5$$

Date/Time	T	$T - T_n$	(a_i)	$\approx x$
06/30/10 06:19 AM	58,117,339	1997	(7,9,9,1,7...)	[0.712394, 0.712402]
06/30/10 06:19 AM	58,117,339	1998	(8,9,9,1,8...)	[0.890461, 0.890469]
06/30/10 06:20 AM	58,117,340	1999	(9,9,9,1,9...)	[0.913367, 0.913375]
06/30/10 06:21 AM	58,117,341	2000	(0,0,0,2,0...)	[0.000183356, 0.000184163]
07/01/10 06:21 AM	58,118,781	3440	(0,4,4,3,0...)	[0.0424811, 0.0424891]
07/26/10 02:43 PM	58,135,312	19971	(1,7,9,9,1,...)	[0.128006, 0.127998]

References

[1] Strogatz, Steven. Nonlinear Dynamics and Chaos. Westview Pr, 2000. pp 343-353 160

[2] GraphicalAnalysis.m Package, By Thomas LoFaro, tlofaro@gustavus.edu. Copyright 2001, Thomas LoFaro