Introduction to Algorithms and Informatics	June 6, 2012
Lecture 8	
Lecturer: David Avis	*Scribe: David Avis*

In this class, we did an experiment using Sudoku to implement Merkle puzzles as a public key distribution scheme. Please see Merkle's account of how his idea was initially rejected [1] and the wiki on Merkle's puzzles [2]. First we consider how to generate a key from a Sudoku game.

1 Keys from Sudoku

We illustrate with 4 X 4 Sudoku games for simplicity. Start with such a game with 5 of the 15 squares filled out. We label the other 10 squares with the variables $k_0, .., k_9$ in row by row fashion.

For example:

k_0	k_1	1	k_2
k_3	k_4	4	3
1	k_5	2	k_6
k_7	2	k_8	k_9

Then the solution to the game

3	4	1	2
2	1	4	3
1	3	2	4
4	2	3	1

gives us a key $K = (3, 4, 2, 2, 1, 3, 4, 4, 3, 1)$. We could use this key in a Vigenère cipher, where each message text letter is shifted in alphabetic order by the appropriate key. So for example the message text M=HELLO WORLD would be encoded C=KINNP XSVOE.

We can imagine Alice and Bob both carry a book of Sudoku puzzles and agree in advance on a certain puzzle number p. Then if Alice wishes to send a message to Bob she can simply solve puzzle p and extract its key K as above. She encodes her message with K and sends it publicly to Bob. Bob can solve also solve puzzle p, get K and decode her message. It requires that both Alice and Bob solve a single Sudoku game. An eavesdropper Eve receiving C would have to brute force solve the puzzles, even if she finds the Sudoku book. If the message M was completely random Eve could never be sure when she had decoded C. Of course Alice does not solve the puzzle by writing directly in the book itself - this would give it away!

2 Merkle's public key distribution based on Sudoku

So far we have seen that a classical key could be generated from a Sudoku game. We will use Merkle's idea to convert this into a public key distribution scheme between Alice and Bob. First we need to compute an identifier for any given key. One way would be to compute a simple hash function, such as $3\sum_{i=0}^{i=4} k_i + \sum_{i=5}^{i=9} k_i$. In this case the identifier would become 3*12+15=51. We assume that this hash function is publicly known.

The protocol for Alice and Bob to agree on a common password M is as follows. We assume that Alice has generated N Sudoku games and published them in a book. Since she knows all the solutions, she can compute a list containing the identifier of each puzzle. We assume she has also deleted any game that would have created a duplicate identifier.

- Bob privately chooses a random Sudoku game from his copy of the book and solves it. He gets a key K and computes its identifier I.
- Bob publicly announces I.
- Alice looks up the identifier I in her list and finds the key K.
- Alice codes up a password M for Bob using K getting code C. She sends C to Bob publicly.
- Bob uses the key K to recover the password M from C
- Alice and Bob communicate using shared password M

As an example, suppose Bob chose the above Sudoku game, getting $K = (3, 4, 2, 2, 1, 3, 4, 4, 3, 1)$ and identifier I=51. He announces I=51 publicly. Alice looks up I in her list and recovers K. She chooses the password M=HELLO WORLD which when encoded by K gives C=KINNP XSVOE. Alice announces C publicly. Bob now uses K to recover M from C by shifting the code letters backwards in alphabetic order. Using M as a key they can communicate privately.

3 Exercises

Many cryptographic schemes have a "trap door", which is a short-cut method to avoid doing a brute force search. The method above admits several such trap-doors. Consider the list of N=8 puzzles below.

(a) Explain how to compute the signature of 7 of the 8 puzzles without solving any of the puzzles at all!

(b) For the remaining puzzle show how to compute its signature by solving for only two empty squares.

(c) Suggest a stronger method of obtaining a signature, and argue why you need to solve each complete puzzle to compute this signature. Compute the signature for each of the eight puzzles.

(d) Explain why M=HELLO WORLD is not a good choice of secret password by Alice. Ie., explain how using simple English text could make Eve's job easier. What is a good choice for Alice?

1

		2	
	1		4
4		1	
	2		

2

	4		
1		2	
	2		3
		4	

3

	2	1	
1			4
	4	3	

4

		4	1
4			
2	3		
			3

www.PrintActivities.com
SUDOKU FOR KIDS: Level 4

page 10 www.PrintActivities.com
SUDOKU FOR KIDS: Level 4

5

			4
4	3		
		1	3
3			

6

		3	
	3		2
3		2	
	4		

7

2			4
		1	
	4		
3			1

8

4			3
		2	
	4		
3			2

References

[1] Merkle's project proposal: http://www.merkle.com/1974/

[2] Merkle's puzzles: http://en.wikipedia.org/wiki/Merkle