3

Rick Staals (0716184)

2WC09- Cryptography 1

Homework sheet 1

September 11, 2013

Question 1

0

The private key in the cryptosystem is a perfect code contained in the public key. Every node in a graph is - by definition - connected to exactly one selected node.

selected nodes are not conn. to selected nodes... ?

Question 2

0

All the nodes in the graph are covered exactly once by the private key. This means that in the public key the values at the nodes in the original private key add up to the sum of the values at all nodes in the original graph.

Question 3

We call the values at the nodes in the message $y_1, \ldots, y_8$ and we call the values at the respective nodes in the original graph $x_1, \ldots, x_8$. We construct an 8×8 matrix M which consists of entries M_{ij} as follows.

$$M_{ij} = \begin{cases} 0, & \text{if node } i \text{ and } j \text{ are not connected,} \\ 1, & \text{if node } i \text{ and } j \text{ are connected.} \end{cases}$$

Furthermore we define $y := \begin{pmatrix} y_1 \\ \vdots \\ y_8 \end{pmatrix}$ and $x := \begin{pmatrix} x_1 \\ \vdots \\ x_8 \end{pmatrix}$.

Then, the values $x_1, \ldots, x_8$ at the nodes in the original graph can be found by solving the system of linear equations $Mx = y$. This results in

2

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} = \begin{pmatrix} 17 \\ 3 \\ -4 \\ 16 \\ 4 \\ 14 \\ 10 \\ 12 \end{pmatrix}.$$

If we solve this system of equations, we get the following result.

why does this work?

$$x = \begin{pmatrix} 4 \\ 5 \\ -3 \\ 6 \\ -7 \\ 4 \\ 5 \\ 9 \end{pmatrix}$$

So the decryption of the message is $4 + 5 - 3 + 6 - 7 + 4 + 5 + 9 = 23$.

Question 4

If we want to break the system for 10000 nodes, we use the same method as in Question ~~4~~ 3. We construct the $y = \begin{pmatrix} y_1 \\ \vdots \\ y_1 0000 \end{pmatrix}$ and $M = \begin{pmatrix} M_{1,1} & \dots & M_{10000,1} \\ \vdots & \ddots & \vdots \\ M_{1,10000} & \dots & M_{10000,10000} \end{pmatrix}$ as described in Question 3.

1

After that, we solve the system $Mx = y$, with $x = \begin{pmatrix} x_1 \\ \vdots \\ x_{10000} \end{pmatrix}$. The decoded message is $\sum_{i=1}^{10000} x_i$.

what if the solution is not unique?
will this method still work?