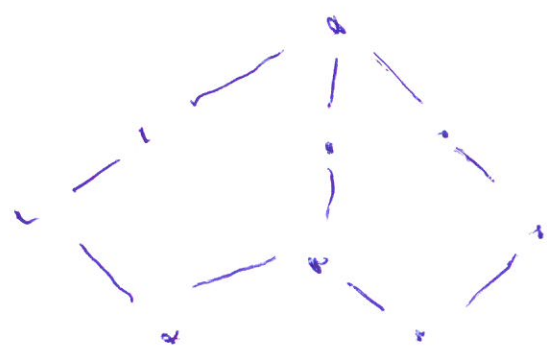
Cryptography

Chapter 1

An Example

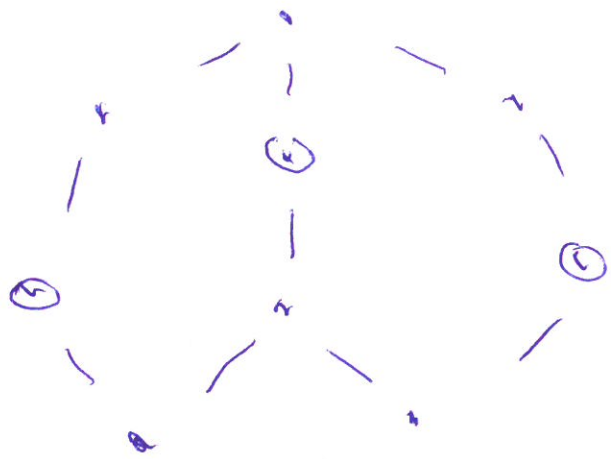
1. We begin by looking at an example that is used for explanation purposes only

A graph consists of a set V of verticies and a set E of edges which join verticies



The graph has 9 verticies and 10 edges. Vertices are neighbors if they are connected by an edge. A graph is perfect if it has a subset S of verticies such that each vertex is in S or is a neighbor of exactly one

element in S. An example is

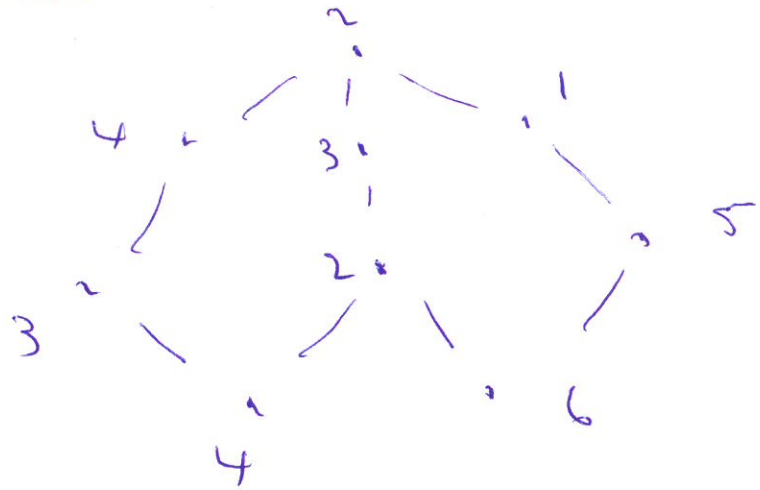


The elements in S are circled.

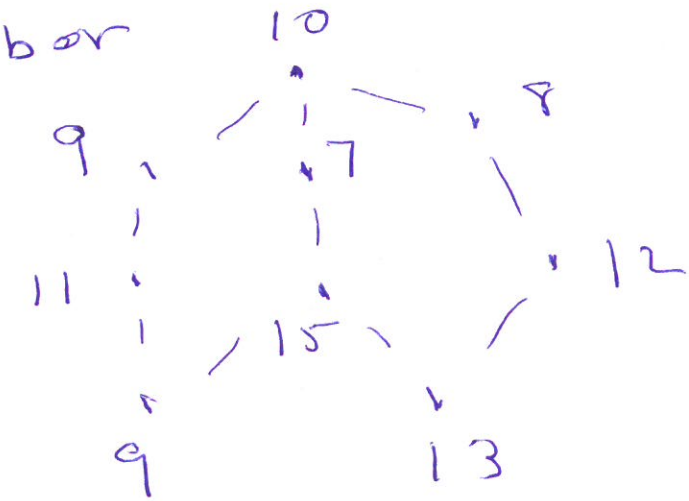
We set up a cryptosystem using perfect graphs. Alice picks a perfect graph and displays it for all to see and use. She does NOT show the special verticies. They are her private key. The graph is her public key

3.

Bob wants to send the message $n = 30$ to Alice. He distributes numbers which add to $n = 30$ to the verticies



Then, for each vertex, he adds the number at the vertex to the numbers at each neighbor



He sends the last graph to Alice. Alice adds the numbers on the special vertices to get n. In our example, that is

$11 + 12 + 7 = 30$

Why does this work?

Terminology:

The special vertices are the private key

The graph is the public key

The graph sent by Bob is the ciphertext

The number $n=30$ is the plaintext

Suppose that Eve is an intruder. She knows the public key and the ciphertext.

but that does not mean that she can find the plaintext (or the private key) If she can, she breaks the system. Note, finding the private key is better for she not only breaks this message but also all other messages sent using this system. Also ~~A~~ Eve also could use this system to send Alice a message

This public key system can have messages sent without the participants meeting to set up the cryptosystem. This is the advantage of public key cryptography, developed in 1976 (unless you count that is was known by the military in WW II but not disclosed

6. Summary. The advantages of public key cryptography

I They can communicate without meeting to set up a key

II Alice has a system that everyone can use to send her messages

Before the public key idea, there was private key cryptography and it has been around virtually forever. Indeed the first system we look at is called the Ceasar Cipher, used by Julius Ceasar.