HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 2



Mehmet Taha USTA – 21527472

Subject: What is the primitive root? Show an example

**Primitive roots**







**On Cryptographic Primitive Roots**

We call primitive roots which are small powers of small primes *cryptographic primitive roots*. Without small primitive roots which are a prime power, a prime may have little cryptographic value for stream ciphers. Thus the distribution of primitive roots has cryptographic importance. This distribution has been investigated by many scholars.