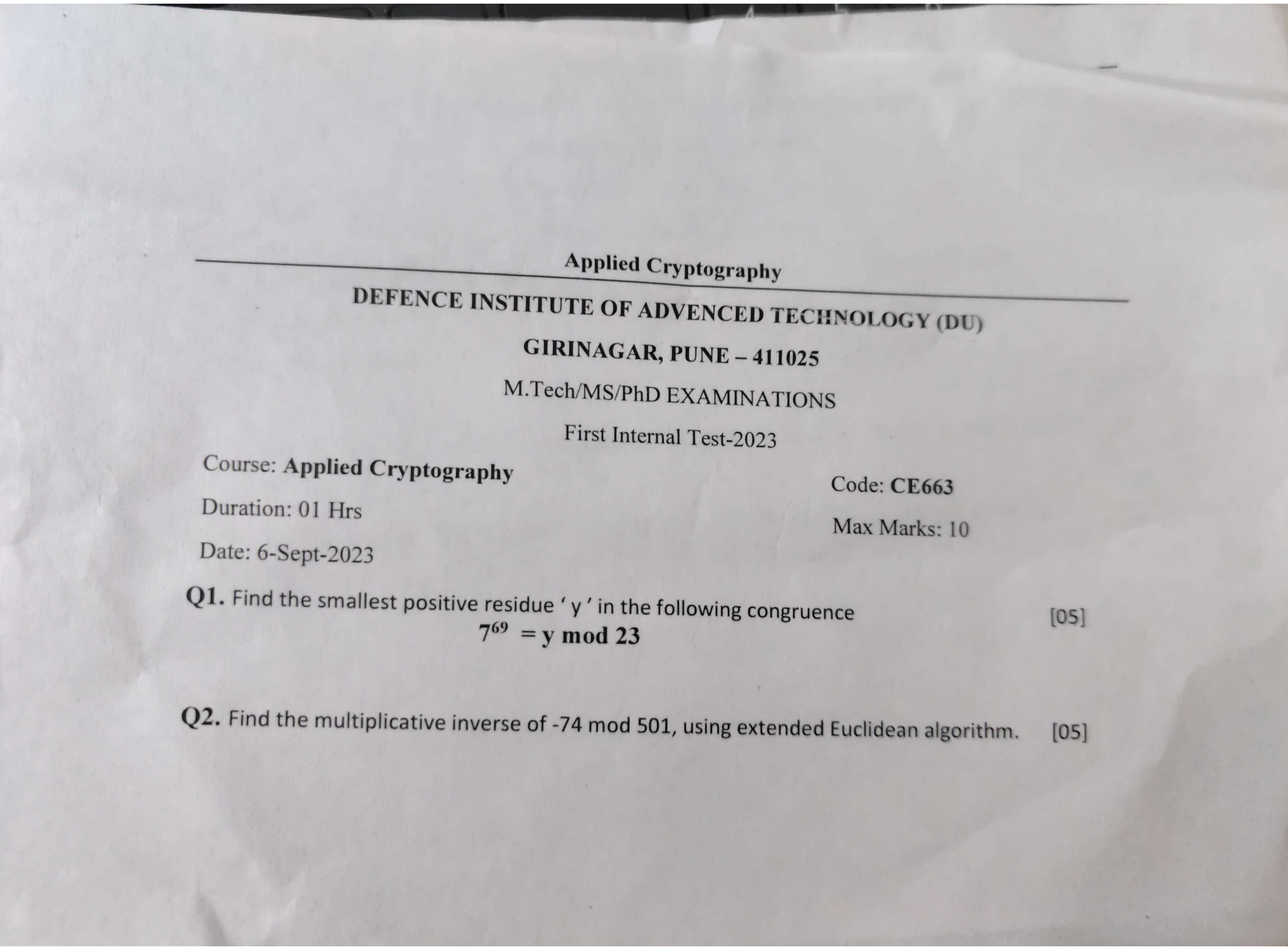


Applied Cryptography

DEFENCE INSTITUTE OF ADVENCED TECHNOLOGY (DU)

GIRINAGAR, PUNE – 411025

M.Tech/MS/PhD EXAMINATIONS

First Internal Test-2023

Course: **Applied Cryptography**

Code: **CE663**

Duration: 01 Hrs

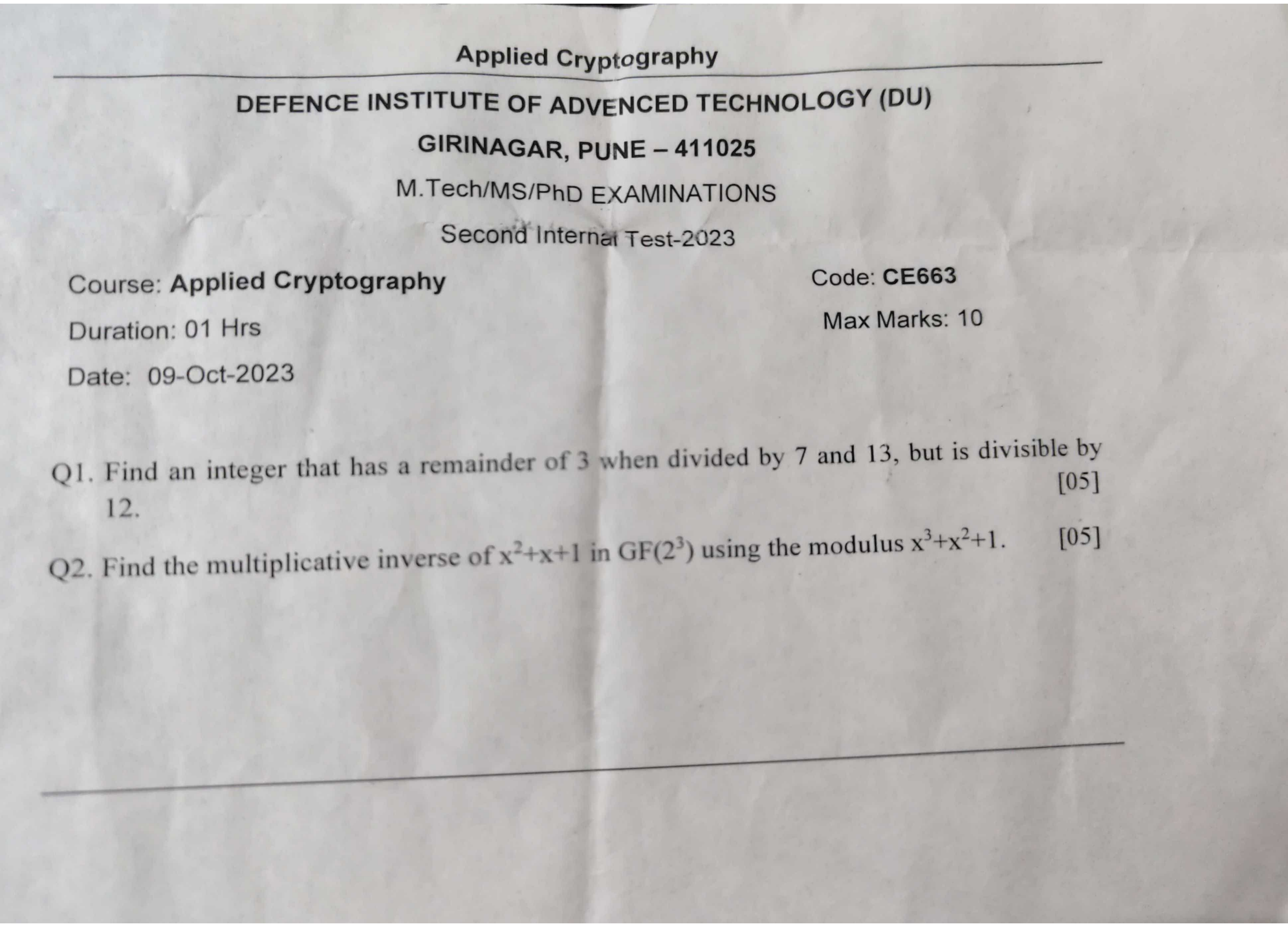
Max Marks: 10

Date: 6-Sept-2023

Q1. Find the smallest positive residue ‘ y ’ in the following congruence [05]

$$\mathbf{7^{69} = y \bmod 23}$$

Q2. Find the multiplicative inverse of -74 mod 501, using extended Euclidean algorithm. [05]



Applied Cryptography

DEFENCE INSTITUTE OF ADVENCED TECHNOLOGY (DU)

GIRINAGAR, PUNE – 411025

M.Tech/MS/PhD EXAMINATIONS

Second Internal Test-2023

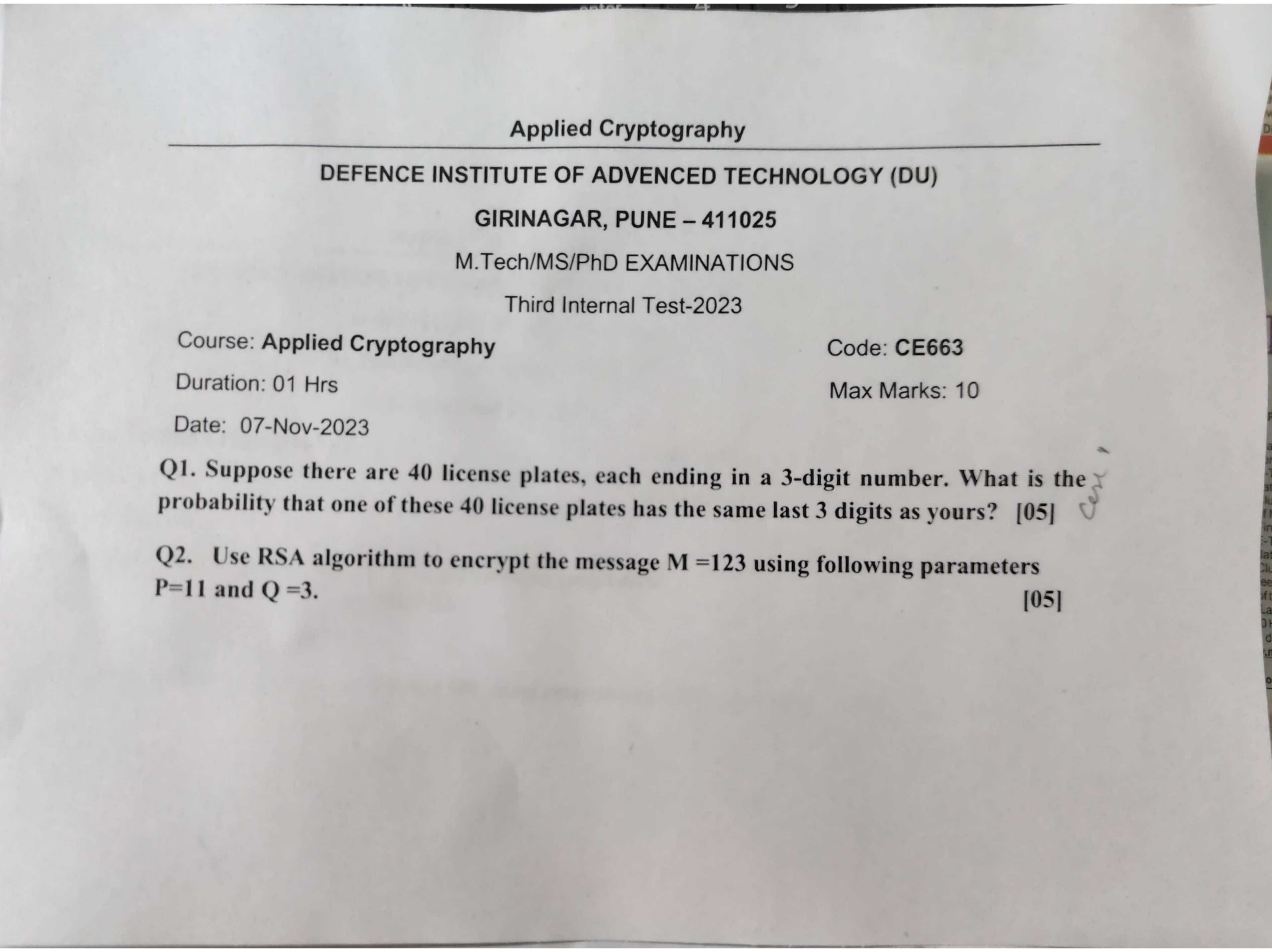
Course: **Applied Cryptography** Code: **CE663**

Duration: 01 Hrs Max Marks: 10

Date: 09-Oct-2023

Q1. Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12. [05]

Q2. Find the multiplicative inverse of x^2+x+1 in $GF(2^3)$ using the modulus x^3+x^2+1. [05]



Applied Cryptography

DEFENCE INSTITUTE OF ADVENCED TECHNOLOGY (DU)

GIRINAGAR, PUNE – 411025

M.Tech/MS/PhD EXAMINATIONS

Third Internal Test-2023

Course: **Applied Cryptography** Code: **CE663**

Duration: 01 Hrs Max Marks: 10

Date: 07-Nov-2023

Q1. Suppose there are 40 license plates, each ending in a 3-digit number. What is the probability that one of these 40 license plates has the same last 3 digits as yours? [05] Cert

Q2. Use RSA algorithm to encrypt the message M =123 using following parameters P=11 and Q =3. [05]