<table>
<tr><td rowspan="3"></td><td colspan="4">Course name: MATH 426
Introduction to Cryptography</td><td colspan="3">Department: Mathematics</td><td>Semester
8</td></tr>
<tr><td colspan="7">Methods of Education</td><td>Credit (ECTS)</td></tr>
<tr><td>Lecture</td><td>Recitation/ (Etud)</td><td>Lab</td><td>Exams</td><td>Homework</td><td>Other</td><td>Total</td><td rowspan="2">6</td></tr>
<tr><td>42</td><td>0</td><td>0</td><td>48</td><td>42</td><td>48</td><td>180</td></tr>
<tr><td>Language</td><td colspan="8">English</td></tr>
<tr><td>Compulsory/Elective</td><td colspan="8">Elective</td></tr>
<tr><td>Prerequisites</td><td colspan="8">Consent of the instructor</td></tr>
<tr><td>Course Contents</td><td colspan="8"><table>
<tr><td>Week</td><td>Subjects</td></tr>
<tr><td>1</td><td>▪ Secure Communications
▪ Cryptographic Applications</td></tr>
<tr><td>2</td><td>▪ Classical Cryptosystems
▪ Shift Ciphers</td></tr>
<tr><td>3</td><td>▪ Affine Ciphers
▪ The Vigenere Cipher</td></tr>
<tr><td>4</td><td>▪ Substitution Ciphers
▪ Sherlock Holmes
▪ The Playfair and ADFGX Ciphers</td></tr>
<tr><td>5</td><td>▪ Block Ciphers
▪ Binary Numbers and ASCII</td></tr>
<tr><td>6</td><td>▪ One-Time Pads
▪ LFSR Sequences</td></tr>
<tr><td>7</td><td>▪ Enigma
▪ A Simplified DES-Type Algorithm</td></tr>
<tr><td>8</td><td>▪ Password Security
▪ Computer Problems</td></tr>
<tr><td>9</td><td>▪ The RSA Cryptosystem</td></tr>
<tr><td>10</td><td>▪ The Knapsack Cryptosystem</td></tr>
<tr><td>11</td><td>▪ Discrete Logarithms</td></tr>
<tr><td>12</td><td>▪ Hash Functions</td></tr>
<tr><td>13</td><td>▪ The Elgamal Public Key Cryptosystem</td></tr>
<tr><td>14</td><td>▪ The Elliptic Curve Cryptosystem</td></tr>
</table></td></tr>
<tr><td>Course Objectives</td><td colspan="8">The purpose of this course is
• to see an overview of cryptography and learn its main applications</td></tr>
<tr><td>Learning Outcomes and Competences</td><td colspan="8">At the and of this course students will
• learn some important real life applications of cryptography</td></tr>
<tr><td>Textbook and /or References</td><td colspan="8">Text book:
Introduction to Cryptography with Coding Theory, Wade Trappe, L.C. Washington, 3rd Edition, Pearson Education, 2020.

References:
Understanding Cryptography, C. Paar, J. Pelzl, Springer, 2010</td></tr>
</table>

Assessment Criteria		If any, mark as (X)	Percentage (%)
	Midterm Exams	X	40
	Quizes		
	Homework		
	Projects		
	Term Paper		
	Laboratory work		
	Other		
	Final Exam	X	60
Instructors			