科目区分・分類	専共・講義	対象学科名・学年	両専攻 2年	科目コード	88921500
科目名	情報セキュリティ論　Information Security Theory				
担当教員	藤澤　義範				
単位数（時間数）	選択　前期　2単位　（30時間）	学習・教育目標との対応	(D-1)		
授業の目的と概要	情報セキュリティの中でも特に重要な技術である暗号技術について主に学習する．暗号技術は，現在のインターネットセキュリティのために開発された技術ではなく，通信全般で利用可能な技術である．暗号方式には，共通鍵暗号方式と公開鍵暗号方式の2種類があり，それぞれについて学習し理解を深める．				
先修科目					
後修科目					
備考	基礎的な整数論について理解していることが望ましい．また，プログラムによる暗号の実装も行うので，プログラミングの知識が不足する場合は各自が事前に補っておくこと．				

	授業項目	時間	内容
1	ネットワークセキュリティの概要	2	ネットワークセキュリティの重要性について理解できる．
2	暗号技術の歴史と概要	2	暗号技術のこれまでの発展の歴史と古典暗号と近代暗号の違いが説明できる．
3	共通鍵暗号方式の概要と分類	2	共通鍵暗号方式の基本となる仕組みや問題点を学び，その仕組みを理解できる．
4	DES暗号方式	2	DES暗号方式について理解できる．
5	IDEA暗号方式	2	IDEA暗号方式について理解できる．
6	プログラムによる共通鍵暗号方式の実装	2	これまでに学習した共通鍵暗号方式の1つをプログラムで実装できる．
7	公開鍵暗号方式の概要と分類	4	公開鍵暗号方式の基本となる数学の諸問題ついて学び，ネットワークセキュリティの実現方法を理解できる．
8	整数論の基礎	2	初歩的な整数論について理解できる．
9	MH暗号方式	2	MH暗号方式ついて理解できる．
10	RSA，Elgamal暗号方式	2	RSA，Elgamal暗号方式について理解できる．
11	プログラムによる公開鍵暗号方式の実装	2	これまでに学習した公開鍵暗号方式の1つをプログラムで実装できる．
12	暗号鍵配送方式	2	暗号鍵の配送技術である DH 法について学習し，鍵配送の仕組みを理解できる．
13	暗号解読法	2	暗号を解読する初歩的な方法について学習し，簡単な暗号を解読できる．
14	前期期末試験	2	

学習・教育目標を達成するために身に付けるべき内容	共通鍵暗号方式と公開鍵暗号方式の違いを仕組みと用途から説明することができ，IDEA暗号方式の原理，RSA暗号方式の原理を説明することができる．これらの内容を満足することで，学習・教育目標の(D-1)の達成とする．
成績評価	前期期末試験（40%），レポート（60%）の合計100点満点で(D-1)を評価する．
教材	教科書：必要に応じてプリントを配布
オフィスアワー	毎週水曜日16:00〜17:00，電子情報工学科1F第二教員室．