Version9- 230627

2023 年度高度セキュリティ PBL/先進セキュリティPBL 授業の流れ　2023/7/1, 7/8-7/9

情報セキュリティ

講師：　宮地 充子,
インストラクター：奥村 伸也,
補助学生:　PoChu Hsu, Ghafoori Nasratullah, DE GOYON Mathieu, CHEN Kaiming,
和泉 海, 上杉 慧至, 田川 雄大, 寺田 誠志郎, 前野 優太, 山下 慎太郎, 山月 達太, He Bingchang,

教科書：　**「代数学から学ぶ暗号理論」**　（日本評論社）　第 2, 3, 4, 5, 7, 8, 10, 13 章 を利用
修得知識：　公開鍵暗号の概念と数論応用の手法の理解，さらに実装に必要な基礎知識
会場：大阪大学吹田キャンパス E1-217（講義及び演習）
TA ミーティング
6/20(火) 13:30～15:00(7/1 練習)，6/21(水)　13:30～(7/8 練習)，6/27(火) 13:30～15:00(7/9 練習)
6/28(水) 13:30～15:00（やりなおし），7/4（火）13:30～15:00
お弁当取りに行く係

6/30(金)　16:30- E1-217 設定
7/1(土)　9:30- 開錠　(担当：Mathieu)
10:00-17:30　吹田キャンパス E1-217
10:00-10:05
演習概要説明 **(講師：宮地)**
10:05-11:00
1.　**演習 0. python で数学を（講師：　奥村)**
(ア)　python を用いて，初等整数論，統計解析などに応用する手法を学習する
11:10-12：10
2.　**講義 1. 暗号の基礎となる整数論及び必要なアルゴリズムの紹介と実装　(教科書第 2 章)**
(ア)　　知識単位：ユークリッドの互除法，バイナリ法
12:10-14:15　**(13:45 -TA による解答)**
3.　演習 1. 有限体の基本アルゴリズムの実験（講義 1）(TA：寺田)
(ア)　　各アルゴリズムの実行時間を調べる
12:30-13:45 記念写真撮影＋lunch 会 1（13:15-）：Memorial photograph
13:45-14:45
4.　講義 2. サイドチャネル攻撃と初等整数論を応用した防御方法（教科書第 3 章)
(ア)　実装による実験解析を実施する
　　知識単位：サイドチャネル攻撃，フェルマーの小定理
14：45-15:30　**(15:00 -　kaiming TA による解答)**
5.　演習 2. サイドチャネル攻撃と初等整数論を応用した防御方法(講義 2)（TA：Kaiming)
15:30-16:00
6.　講義 3. 公開鍵暗号の概念及び ElGamal 暗号の紹介と実装（教科書 8 章)
(イ)　知識単位：公開鍵暗号の概念，ElGamal 暗号，鍵共有の概念，DH 鍵共有法
16:00-17:00　**(16:30-　和泉，前野　TA による解答)**
7.　演習 3-1. ElGamal 暗号の構成（講義 3）(TA：和泉)
8.　演習 3-2. DH 応用（講義 3）　(TA：前野)
(ウ)　公開鍵を掲示板に登録，秘密通信ゲームの実施.
17:00-17:30
9.　講義 4-1. 典型的な解読方法 ρ 法とその実装，並列化(教科書 12 章)　(Nas)
(ア)　　知識単位：ρ 法，指数計算法鍵

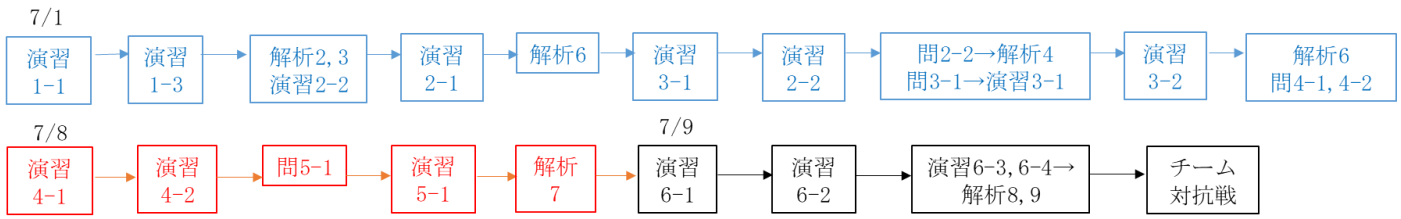
7/8（金）16:30- E1-217 設定
7/9（土）9:30- 開錠　(担当：Mathieu)
7/9（土）10:00-18:15 吹田キャンパス E1-217
10:00-10:30
11. 演習 2-2. 乱数の精度（講義 2）（10:00- TA:上杉)
12. 演習 4-1.　典型的な解読方法 ρ 法とその実装，並列化(講義 4)（10:15- TA：田川)

10:30-11:30
10.　講義 4-2.　公開鍵暗号の応用　(Hsu)
（ア）　知識単位：鍵共有の概念，DH 鍵共有法，暗号の評価手法
（イ）　グループ課題
11:30-12:30
14. 講義 5. ディジタル署名の概念及 DSA 署名の紹介と実装
（ア）　知識単位：ディジタル署名の概念，DSA 署名
12:30-13:40 記念写真撮影＋lunch 会 2（13:20-）：Memorial photograph
13:40-14:10
15. 演習 5. ディジタル署名の概念及 DSA 署名の紹介と実装（講義 6）(14:30- TA：Mathieu)
14:10-15:10
16. 講義 6. ハイブリッド暗号の実装と評価
（ア）　ハイブリッド暗号
　　知識単位：文字コード，暗号と署名の組み合わせ，ハイブリッド暗号暗号プロトコルや署名の応用
15:20-15:50
15. 演習 5. ディジタル署名の概念及 DSA 署名の紹介と実装（講義 6）(15:30- TA：Mathieu)
15:50-17:30
17. 演習 6-1. ハイブリッド暗号の実装と評価（講義 8）(17:00- TA：山月)
17:30-18:30
18. チーム対抗戦議論

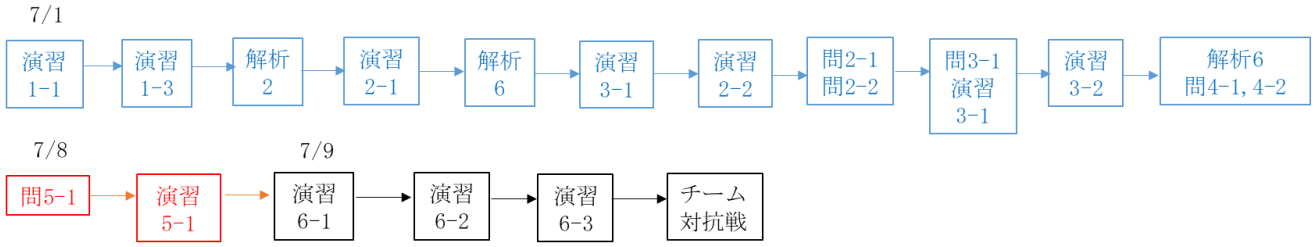
7/10（日） 9:30- 開錠（担当：Mathieu)
7/10（日） 10:00-17:30 吹田キャンパス E1-217
10:00-11:45
13. 演習 4-2　公開鍵暗号の応用講義 5)（TA：山下）
19. 演習 6-2. ハイブリッド暗号の実装と評価（講義 8）(11:15- TA：He)
11:45-13:00 記念写真撮影＋lunch 会 2（12:50-）：Memorial photograph
13:00-14:20
20. チーム対抗戦
14:20-15:50
21. 最終課題発表（15 分×6=90 分）とチーム課題解説（16:00- Hsu，16:20- Nas）
16:50-17:20
22. まとめ　(プロジェクタ)
講義 0. 暗号の原理：暗号の実用例，共通鍵暗号，公開鍵暗号（Projector）
23. Closing Ceremony
23-1. 参加者感想
We wish to thank attendees for their interest to the information security and our laboratory.
宮地研究室の情報セキュリティのアクティビティに参加頂き，ありがとうございました.
23-2. TA 謝辞: PoChu Hsu，Ghafoori Nasratullah，DE GOYON Mathieu，CHEN Kaiming，
和泉 海，上杉 慧至，田川 雄大，寺田 誠志郎，前野 優太，山下 慎太郎，山月 達太，He Bingchang，
We wish to thank 2nd-grade-master students，PhD-candidate students of Miyaji lab for their helping the PBL as TA.
PBL の準備・TA として協力に感謝します.
23-3. インストラクター謝辞: 奥村 伸也
We wish to thank Prof. Okumura for their helping the PBL as instructors.
PBL の準備・インストラクターとして協力に感謝します.
23-4. 謝辞：　宮地 充子
We wish to thank Prof. Miyaji for her holding an annual PBL and continued effort and support in progressing the PBL.
企画立案，開催，準備，講師としてのアクティビティに感謝します.
23-5. 記念写真撮影： Memorial photograph
23-6. アンケート記入： We would like to have your comments.

演習プラン

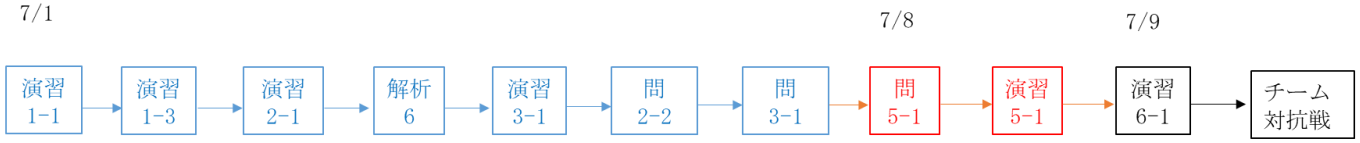
・Advanced Course



・Standard Course



・Basic Course



{参加者名簿}

講師: 宮地 充子, インストラクター :奥村 伸也

TA:PoChu Hsu, Ghafoori Nasratullah, DE GOYON Mathieu, CHEN Kaiming,

和泉 海, 上杉 慧至, 田川 雄大, 寺田 誠志郎, 前野 優太, 山下 慎太郎, 山月 達太, He Bingchang,

参加者: 29 人

社会人(P): 4 人

・安立 征大, 森 毅, 宮城 俊吾, 佐藤 友則,

大学院生(S):15人

・大阪大学大学院工学研究科 10 人: 中島 克也, Wei Pengxuan, 岡田 健汰, 川原 尚己, 佐藤 克洋, 田村 昴輔, 長井 厚樹, 林田 幸大, 東 龍之介, 廣瀬 健二朗, 船津 颯介, 白石 智裕, 水野 伸哉,

・大阪大学大学院情報科学研究科 1 人: 小脇 修和,

・JAIST 1人: 雨宮 岳,

学部生(B):10 人

・大阪大学工学部通信 6 人: 石森 大路, 岡田 侑里英, 柴田 紗由美, 峰田 敏行, 森園 涼斗, 柳下 智史, 山田 麟太郎

・大阪大学工学部情シス1人: 西尾 達也

・大阪大学工学部電子 1 人: 能浦 奈々

・石川高専 1 人: 樋口 実紗,

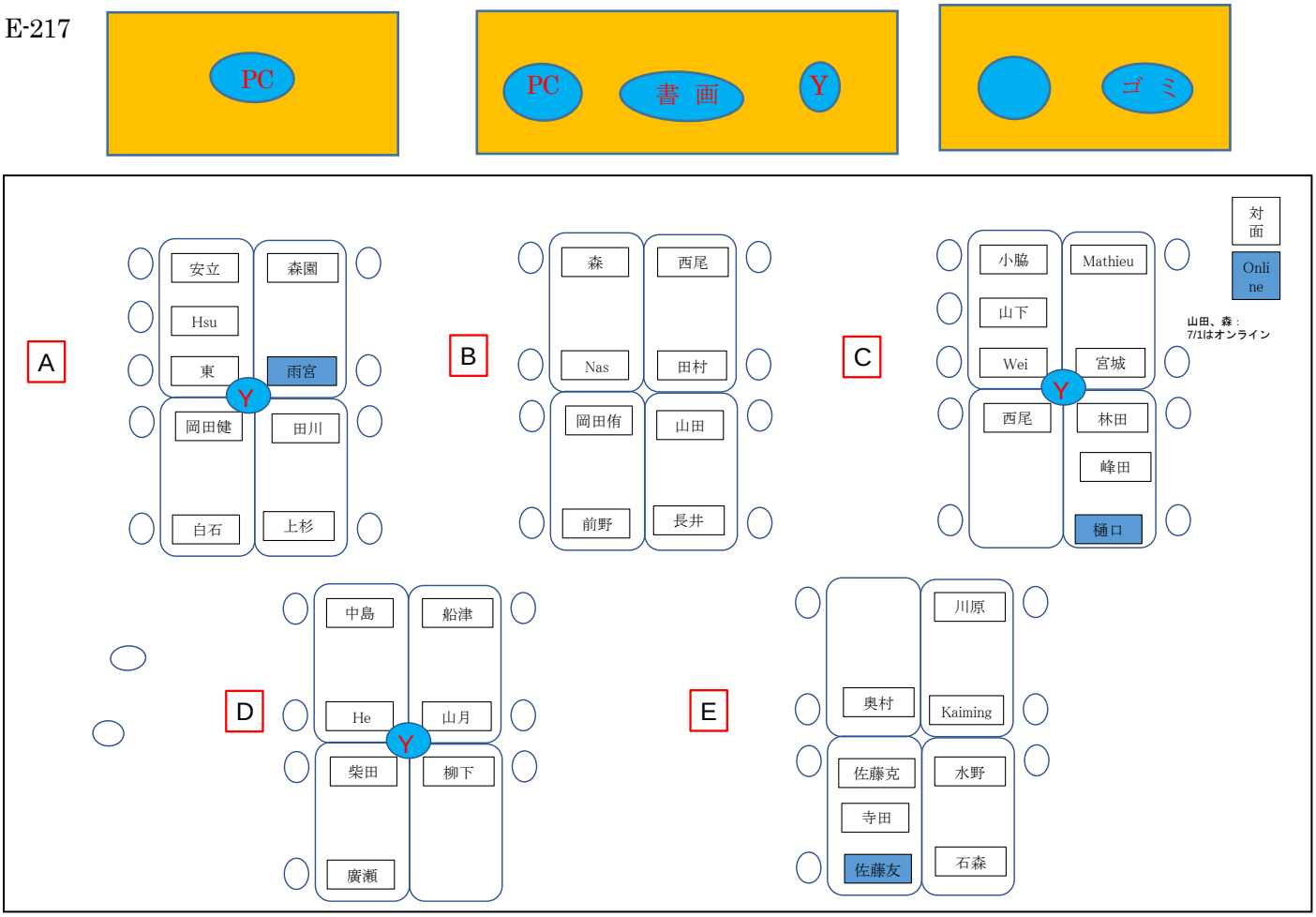
インストラクター・TA 対応表

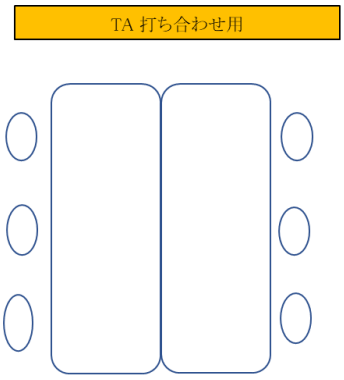
チーム名	生徒番号	所属	受講者	講師, TA	講義1	講義2	講義3	講義4	講義5	講義6	講義7	講義8	Online /対面
チームA 6人	000001	社会人	安立 征大	上杉									
	000010	阪工研	東 龍之介	田川									
	000011	阪工研	岡田 健汰	Hsu									
	000100	阪工量	白石 智裕	Hsu									
	000101	JAIST	雨宮 岳	田川									
	000111	阪工通	森園 涼斗	上杉									
チームB 5人	001001	社会人	森 毅	前野									
	001010	阪工研	田村 昴輔	Nas									
	001011	阪工研	長井 厚樹	Nas									
	001101	阪工通	岡田 侑里英	Nas									
	100110	阪工通	西尾 達也	前野									
	100111	阪工通	山田 麟太郎	前野									
チームC 6人	010001	社会人	宮城 俊吾	山下									
	010010	阪工研	Wei Pengxuan	和泉									
	010011	阪工研	林田 幸大	Mathieu									
	010100	阪基礎	小脇 修和	Mathieu									
	011100	阪工通	峰田 敏行	山下									
	010101	石川高専	樋口 実紗	和泉									
チームD 5人	011001	阪工研	中島 克也	He									
	011010	阪工研	船津 颯介	He									
	011011	阪工研	廣瀬 健二朗	He									
	011101	阪工電	柳下 智史	山月									
	011110	阪工通	柴田 紗由美	山月									
チームE 6人	100001	社会人	佐藤 友則	奥村									
	100010	阪工研	川原 尚己	Kaiming									
	100011	阪工研	佐藤 克洋	寺田									
	100100	阪工量	水野 伸哉	Kaiming									
	100110	阪工通	能浦 奈々	奥村									
	001110	阪工通	石森 大路	寺田									

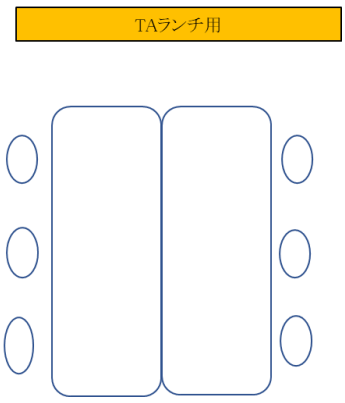
区分：B(学部), S(院), P(社会人)

座席配置

E-217


PC
PC
書 画
Y
ゴ ミ
対面
Online
山田、森：
7/1はオンライン
A
安立
森園
Hsu
東
雨宮
Y
岡田健
田川
白石
上杉
B
森
西尾
Nas
田村
岡田侑
山田
前野
長井
C
小脇
Mathieu
山下
Wei
宮城
Y
西尾
林田
峰田
樋口
D
中島
船津
He
山月
Y
柴田
柳下
廣瀬
E
川原
奥村
Kaiming
佐藤克
水野
寺田
佐藤友
石森


TA 打ち合わせ用


TAランチ用

PBL の準備
1. 担当の課題を回答, プログラム, PPT の解答説明資料の作成
2. 公開鍵の作成, moodle 掲示板に設置
3. Slack チームのとりまとめ. (自己紹介)
4. 事前課題, チーム学生の質問

PBL の当日
1. 各チームの進捗確認.
2. 遅れている学生のフォロー
3. 演習ソフトの API の確認, 指導
4. チームプレゼンの PPT の作成指導, google ppt で共有して作成.
5. チームメンバとのインタラクティブ課題の担当

PBL 後
1. 提出課題の確認. (python API の確認)
2. 問の確認

Preparation for PBL
1. answer assignments, create programs and PPTs to explain answers
Create a public key and put it on the moodle board.
3. Organize the Slack team. (Self-introduction)
4. preliminary assignments, questions from team students

Day of PBL
1. Check the progress of each team.
2. Follow-up on students who are behind.
3. Checking the API of the exercise software and guidance
4. Instruction on making PPTs for team presentations, shared via google ppt.
5. Responsible for interactive assignments with team members

After PBL
1. Confirmation of submitted assignments. (Confirmation of python API)
2. Confirmation of questions

Translated with www.DeepL.com/Translator (free version)