情報セキュリティ関係者を対象とした

「暗号講座」 開催のご案内

暗号は、ICT社会の基盤であり、情報セキュリティにとって基盤技術であるにもかかわらず、暗号研究者・技術者以外には、難解に感じられているようであり、安全性の高い暗号の選択法や運用法に関しては、情報セキュリティの専門家ですら知識と理解が足りないのが現状である。
本講座では、暗号の正しい利用と普及に向けて、情報セキュリティ関係者、暗号数理に興味を持つ学生などを対象に、暗号技術の初歩から国際標準化の現状、暗号に関する社会制度、電子商取引、電子政府、電子投票・アンケートなど様々な分野での応用などを、第一線の研究者・専門家がじっくり時間をかけて丁寧に解説する。

●主催：文部科学省科学技術振興調整費
中央大学研究開発機構「情報セキュリティ・情報保証　人材育成拠点」

●開講スケジュール

開催日：2007 年 7 月～2008 年 3 月の各月の土曜日 (詳細は下記のとおり)　全 15 回

時間：毎回　前半 13:30～15:00　後半 15:10～16:40　(受付開始 13:00)

●会場：中央大学後楽園キャンパス 3 号館

●受講費無料

●プログラム (**プログラムは、変更されることもありますので、あらかじめご承知おきください。**)

2007 年　　（敬称略）

7 月 14 日 (土)	歴史を変え、情報社会を拓いた暗号	情報セキュリティ大学院大学学長 辻井　重男 大阪学院大学情報学部教授 笠原　正雄
21 日 (土)	暗号理論入門―整数論の初歩	中央大学研究開発機構准教授 只木　孝太郎
28 日 (土)	暗号理論入門―素因数分解とＲＳＡ暗号	山形大学工学部教授 小林　邦勝 金沢工業大学工学部教授 林　彬
8 月 4 日 (土)	暗号理論入門―離散対数問題とエルガマル暗号	只木　孝太郎
25 日 (土)	共通鍵暗号の基礎	東京理科大学理工学部教授 金子　敏信 株式会社富士通研究所 セキュアコンピューティング研究部 下山　武司
9 月 1 日 (土)	共通鍵暗号の開発と利用動向	ソニー株式会社 情報技術研究所 盛合　志帆 三菱電機株式会社 情報技術総合研究所 松井　充
8 日 (土)	安全性証明・鍵共有	ＮＴＴ情報流通プラットフォーム研究所 岡本　龍明 情報セキュリティ大学院大学教授 有田　正剛
29 日 (土)	ハッシュ関数とその応用	福井大学大学院工学研究科准教授 廣瀬　勝一 株式会社日立製作所 システム開発研究所 寶木　和夫

10 月 6 日 (土)	楕円曲線暗号の基礎	中央大学理工学部教授 趙 晋輝 情報セキュリティ大学院大学教授 松尾 和人

2008 年

1 月 19 日 (土)	(前半) 暗号プロトコル入門 (後半) 電子投票と暗号プロトコル	情報セキュリティ大学院大学教授 土井 洋 中央大学研究開発機構教授 山口 浩
2 月 2 日 (土)	暗号利用モードとその標準化動向	茨城大学工学部教授 黒澤 馨 名古屋大学大学院工学研究科准教授 岩田 哲
9 日 (土)	(前半) CRYPTREC の活動 (後半) ISO 等の国際標準化の動向	中央大学理工学部教授 今井 秀樹 横浜国立大学大学院環境情報研究科教授 松本 勉 九州大学大学院ｼｽﾃﾑ情報科学研究院教授 櫻井 幸一 北陸先端科学技術大学院大学 情報科学研究科准教授 宮地 充子
23 日 (土)	サイドチャネル攻撃の耐タンパー性	日本電気株式会社 共通基盤ソフトウェア研究所 主席研究員 角尾 幸保 独立行政法人情報処理推進機構 セキュリティセンター暗号グループリーダー 山岸 篤弘
3 月 1 日 (土)	(前半) システムから見た暗号利用と鍵管理 (後半) 電子商取引･金融分野における暗号利用	NTT 情報流通プラットフォーム研究所 神田 雅透 日本銀行金融研究所 情報技術研究センターセンター長 岩下 直行
15 日 (土)	パネル討論会 暗号技術の発展と普及に向けて	パネリスト 中央大学理工学部教授 今井 秀樹 電気通信大学情報通信学部教授 太田 和夫 筑波大学電子･情報工学系教授 岡本 栄司 株式会社東芝 研究開発ｾﾝﾀｰ研究主幹 川村 信一 東京電機大学工学部教授 佐々木 良一 NTT 情報流通プラットフォーム研究所 青木 和麻呂 コーディネータ 大阪学院大学情報学部教授 笠原 正雄 情報セキュリティ大学院大学学長 辻井 重男

●受講申し込み方法

1）受講申込みは、準備の都合上原則として前もってお申込みください。

2) 必要事項 (ご氏名･勤務先(大学名)･参加希望日) をご記入のうえお申し込みください。

プログラム詳細･参加お申込み先 ： crypt2007@tamajs.chuo-u.ac.jp