

「暗号講座」 開催のご案内

●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月15日のみ、中央大学駿河台記念館)

●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) 5号館 5134号室	(前半)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
	(後半)歴史を変え、情報社会を拓いた暗号 —テクノロジーと数学のかかわりの歴史を鳥瞰し、 暗号技術の将来を考える—	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 (前半)素因数分解に関して	山形大学工学部教授 小林 邦勝
	(後半)RSA入門	金沢工業大学工学部教授 林 彬
8月4日(土) 6号館 6401号室	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) 6号館 6401号室	共通鍵暗号の基礎	東京理科大学理工学部教授 金子 敏信
	暗号用擬似乱数の安全性評価 — ストリーム暗号 MUGI の安全性 —	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) 6号館 6401号室	共通鍵暗号の開発と利用動向 DES、AESからCLEFTIAまで	ソニー株式会社 情報技術研究所 盛合 志帆
	Linear Cryptanalysis of Block Ciphers (ブロック暗号の線形解読法)	三菱電機株式会社 情報技術総合研究所 松井 充
8日(土) 6号館 6401号室	暗号安全性証明	NTT 情報流通プラットフォーム研究所 岡本 龍明
	認証と鍵共有プロトコル	情報セキュリティ大学院大学教授 有田 正剛
29日(土) 5号館 5138号室	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
	ハッシュ関数とその応用(2) —認証、鍵配送、コミットメント付与、ポスト量子計算他—	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) 5号館 5138号室	楕円曲線暗号の基礎	中央大学理工学部教授 趙 晋輝
	楕円曲線暗号の基礎 2	情報セキュリティ大学院大学教授 松尾 和人

2008年

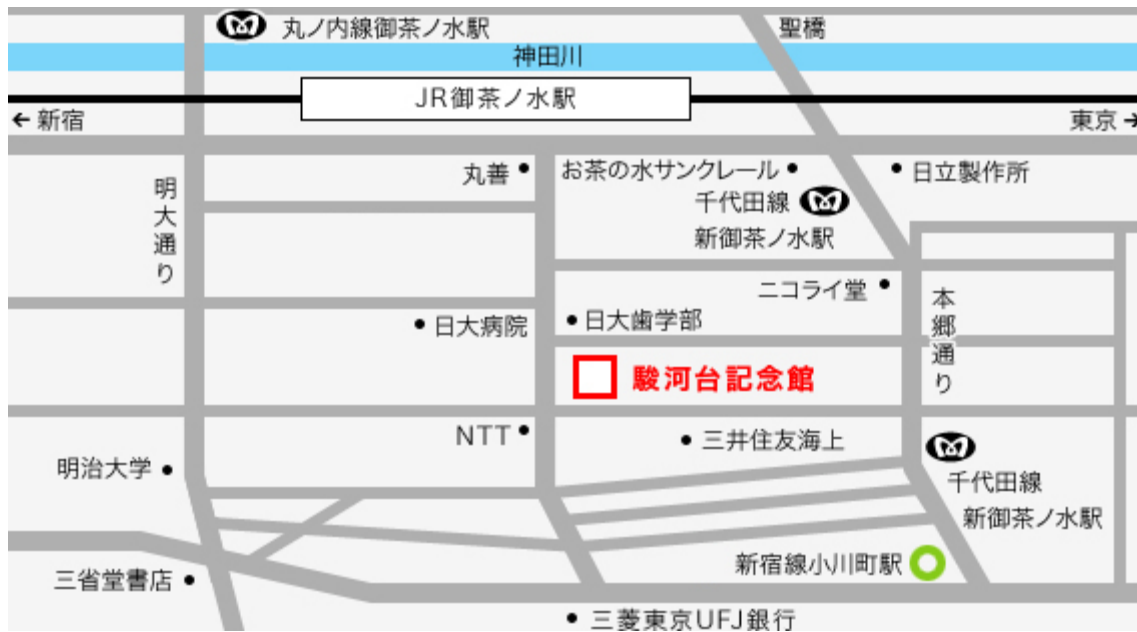
1月19日(土) 6号館 6401号室	暗号プロトコル入門	情報セキュリティ大学院大学教授 土井 洋
	電子投票と暗号プロトコル	中央大学研究開発機構教授 山口 浩
2月2日(土) 6号館 6301号室	暗号利用モードとその標準化動向 1	茨城大学工学部教授 黒澤 馨
	暗号利用モードとその標準化動向 2	名古屋大学大学院工学研究科准教授 岩田 哲
9日(土) 6号館 6301号室	CRYPTREC の活動	中央大学理工学部教授 今井 秀樹 横浜国立大学大学院環境情報研究院教授 松本 勉
	情報セキュリティの標準化動向について Current Status on Standardization of Cryptographic Technologies	北陸先端科学技術大学院大学情報科学研究科教授 宮地 充子 九州大学大学院システム情報科学研究院教授 櫻井 幸一
23日(土) 5号館 5234号室	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) 5号館 5234号室	(前半) システムから見た暗号利用と鍵管理	NTT 情報流通プラットフォーム研究所 神田 雅透
	(後半) 電子商取引・金融分野における暗号利用	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) 中央大学 駿河台記念館 280号室 (記念館へのアクセス は次ページ)	10:30 — 12:00 ストリーム暗号	神戸大学大学院 工学研究科教授 森井 昌克
	13:30 — 16:40 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

● 受講申込方法

- 1) 受講申込は、準備の都合上事前にお申込ください。
- 2) 必要事項(ご氏名・勤務先名または大学名・受講希望日)をご記入に上お申込ください。

受講申込先：crypt2007@tamaja.chuo-u.ac.jp

中央大学駿河台記念館



東京都千代田区神田駿河台 3-11-5

tel:03-3292-3111 (記念館事務室)

JR 中央・総武線 御茶ノ水駅下車 徒歩 3 分

東京メトロ丸ノ内線 御茶ノ水駅下車 徒歩 6 分

東京メトロ千代田線 新御茶ノ水駅下車 (B1 出口) 徒歩 3 分

都営地下鉄新宿線 小川町駅下車 (B5 出口) 徒歩 5 分

http://www.chuo-u.ac.jp/chuo-u/access/access_surugadai_j.html