bilimsel program
scientific programme

1. gün
first day
25 Aralık December **2008**
Perşembe Thursday

	KEMAL KURDAŞ SALONU	A SALONU	B SALONU	D SALONU
09:00 - 10:00	**KAYIT** REGISTRATION			
10:00 - 10:45	**AÇILIŞ TÖRENİ** OPENING CEREMONY Prof. Dr. Şeref SAĞIROĞLU Bilgi Güvenliği Derneği Başkanı Prof. Dr. Ahmet ACAR ODTU Rektörü Prof. Dr. Rıza AYHAN Gazi Üniversitesi Rektörü Dr. Tayfun ACARER Bilgi Teknolojileri ve İletişim Kurumu Başkanı Sn. Binali YILDIRIM Ulaştırma Bakanı			
10:45 - 11:00	**ÇAY/KAHVE ARASI** TEA / COFFEE BREAK			
11:00 - 13:00	**PANEL I** **Bilgi Teknolojileri ve İletişim Güvenliği Oturumu** **Panel Başkanı:** Galip ZEREY, Bilgi Teknolojileri ve İletişim Kurumu II. Başkanı Süreyya CİLİV, TURKCELL Selçuk KARAÇAY, VODAFONE Doç. Dr. Turan MENTEŞ, Türkiye Bilişim Derneği Prof. Dr. Şeref SAĞIROĞLU, Bilgi Güvenliği Derneği Tuğrul TEKBULUT, TÜBİSAD Cüneyt TURKTAN, AVEA			
13:00 - 14:00	**ARA** BREAK			
14:00 - 16:00	**PANEL II** **Kişisel Verilerin Korunması** **Panel Başkanı:** Leyla KESER, Bilgi Üniversitesi Nilgün BAŞALP, Bilgi Üniversitesi Elif KUZECİ, Başkent Üniversitesi Kemal DEMİRDÖN, Cumhuriyet Baş Savcı Vekili Volkan SIRABAŞI, Kamu İhale Kurumu	**Oturum 1: ÜLKE BİLGİ GÜVENLİĞİ** Oturum Başkanı: Taner ALTUNOK KHO Savunma Bilimleri Enstitüsü	**Oturum 2: STEGANOGRAFİ** Oturum Başkanı: Ferruh ÖZBUDAK ODTÜ, Uygulamalı Matematik Enstitüsü Matematik Bölümü	**Oturum 3: KRİPTOGRAFİ - 1** Oturum Başkanı: Ali DOĞANAKSOY ODTÜ, Uygulamalı Matematik Enstitüsü Matematik Bölümü
14:00 - 14:20	27 **E- Devlet Güvenliği** Ayşe INALÖZ, Mustafa ÜNVER, Mustafa ALKAN		35 **Bir Steganografi Sisteminin FPGA Üzerinde Gerçeklenmesi** Betül ELÇİ, Berna ÖRS, Volkan DALMIŞLI	68 **Pairing-Based Cryptography: A Survey** Sedat AKLEYLEK, Barış B. KIRLAR, Ömer SEVER, Zaliha YÜCE
14:20 - 14:40	24 **Ülke Bilgi Güvenliği** Yılmaz VURAL, Şeref SAĞIROĞLU		25 **Doğruluk Oranı İyileştirilmiş (2, n) Olasılıklı Görsel Sır Paylaşma Şeması** Vasif NABİYEV, Mustafa ULUTAŞ, Güzin ULUTAŞ	28 **An Analysis of the Generalized ID-Based ElGamal Signatures** Hatice KOYUNCU, Kamer KAYA, Ali Aydın SELÇUK
14:40 - 15:00	76 **Türkiye'de Siber Güvenlik Yönetimine Yönelik Kurumsal Bir Yapılanma Önerisi** Türksel Kaya BENSGHIR, Sema Önal ALTINSOY		45 **Verileri Nota Kullanarak Şifreleme ve Ses Dosyası İçerisine Gizleme** Muhammet YAVUZ, Oğuz ERGİN	50 **Efficient Multiplication in Finite Fields of Characteristic 3 and 5 for Pairing Based Cryptography** Murat CENK, Ferruh ÖZBUDAK
15:00 - 15:20	23 **Security of Critical Information Infrastructures: E-Governance and Standardization** Serap ATAY, Marcelo MASERA		74 **İGS Tabanlı Yeni Bir Video-Sırörtme Yöntemi** Özdemir ÇETİN, Ahmet ÖZCERİT	62 **Arithmetic on Pairing- Friendly Fields** Sedat AKLEYLEK, Barış B. KIRLAR, Ömer SEVER, Zaliha YÜCE
16:00 - 16:20	**ÇAY/KAHVE ARASI** TEA / COFFEE BREAK			

bilimsel program
scientific programme

1. gün
first day
25 Aralık December **2008**
Perşembe Thursday

	KEMAL KURDAŞ SALONU	A SALONU	B SALONU	D SALONU
16:20 - 18:00	**Eğitim I** **KRİPTOLOJİNİN TEMELLERİ ve ELEKTRONİK İMZA ALTYAPISI** Eğitmenler: Sedat AKLEYLEK Begül BİLGİN Erdener UYAN Oğuz YAYLA ODTÜ, Uygulamalı Matematik Enstitüsü	**KURUMSAL SUNUMLAR**	**Oturum 4: GÜVENLİK ALGORİTMALARI** Oturum Başkanı: Emrah ÇAKÇAK ODTÜ, Uygulamalı Matematik Enstitüsü	**Oturum 5: KRİPTOGRAFİ - 2** Oturum Başkanı: Melek D. YÜCEL ODTÜ, Uygulamalı Matematik Enstitüsü Elektrik ve Elektronik Mühendisliği Bölümü
16:20 - 16:40		16:20-17:20 EGÜVEN Elektronik Bilgi Güvenliği A.Ş. **"E-imzada Güvenlik Boyutu ve Uygulamalar"** Alpaslan BİNİCİ	5 **Secure Homogeneous Matrix Algebra via Oblivious Polynomial Evaluation** Mert ÖZARAR, Atilla ÖZGİT	29 **Threshold Cryptography Based on Blakley Secret Sharing** İlker BOZKURT, Kamer KAYA, Ali A. SELÇUK, Ahmet GÜLOĞLU
16:40 - 17:00			11 **Survey on Transformation Based Algorithms in Digital Image Watermarking** Ersin ELBAŞI	56 **Extended Results for Independence and Sensitivity of NIST Randomness Tests** Ali DOĞANAKSOY, Barış EGE, Köksal MUŞ
17:00 - 17:20			22 **Encryption With First Order Splines** Alla LEVINA, Yuri DEMJANOVICH	42 **Alternative Approach to Maurer's Universal Statistical Test** Ali DOĞANAKSOY, Cihangir TEZCAN
17:20 - 17:40			69 **SEA Şifreleme Algoritması Kullanarak Güvenli Kablosuz Algılayıcı Ağ Haberleşmesinin Gerçekleştirilmesi** Cüneyt BAYILMIŞ, Murat ÇAKIROĞLU	52 **Variant Constructions for TMTO Based on Random Mapping Statistics** Nurdan SARAN, Ali DOĞANAKSOY
17:40 - 18:00			80 **Genetik Algoritma Kullanarak Görüntü Kaynaştırma Tabanlı Görünür Damgalama** Veysel ASLANTAŞ, Rıfat KURBAN	
19:00	**KOKTEYL** COCKTAIL			

POSTER ALANI

Oturum 6:
POSTER OTURUMLARI
POSTER PAPERS
Saat: 14:00 - 18:00

60 **Kriptografik Modüllerin Güvenlik Gereksinimleri**
Oğuz YAYLA

53 **Privacy Impact Assessment Methodologies for Protection of Personal Data**
Okyar TAHAOĞLU, Yalçın ÇEBİ

49 **Siber Savunma : Ülkeler ve Stratejiler**
Mehmet MERAL

78 **Türk Patent Enstitüsü E-imza Uygulamaları**
Mustafa ÖZLÜ

26 **Secure Embedding Communication Channels: Exploring Simulated Quantum Electro Dynamic Systems**
Najib SAYLANI

73 **Saldırı Tespit Sistemleri Üzerine Bir İnceleme**
Esra Nergis GÜVEN, Şeref SAĞIROĞLU

77 **E-Sağlık / Tele Sağlık Yönetişiminde Uzaktan Eğitim ve Güvenli Bilgi Yönetim Sistemleri**
Akın MAŞRAP

1 **Elektronik Ticarette Güvenlik İlkeleri**
Tolga MATARACIOĞLU, Ünal TATAR

BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC turkey

bilimsel program
scientific programme

2. gün
second day
26 Aralık December **2008**
Cuma Friday

	KEMAL KURDAŞ SALONU	A SALONU	B SALONU	C SALONU	D SALONU
09:20 - 11:00	**Eğitim II** **KRİPTOGRAFİK ALGORİTMA ve MODÜLLERİN TEST, VALİDASYON ve SERTİFİKASYON SÜRECİ** Eğitmen: Ahmet Hasan KOLTUKSUZ İzmir Yüksek Teknoloji Enstitüsü	KURUMSAL SUNUMLAR	**BTK Özel Oturumu** Oturum Başkanı: Ahmet Hamdi ATALAY BTK Kurul Üyesi	**Oturum 7: KRİPTOANALİZ** Oturum Başkanı: Ali Aydın SELÇUK Bilkent Üniversitesi, Bilgisayar Mühendisliği Bölümü	**Oturum 8: AĞ GÜVENLİĞİ** Oturum Başkanı: Ertuğrul KARAÇUHA Bilgi Teknolojileri ve İletişim Kurumu Başkan Yardımcısı
09:20 - 09:40			**"Kurumlar Arası Elektronik/ Mobil İmzalı Belge Paylaşımı"** Demet KABASAKAL, Bilişim Uzmanı	**38 A Survey of the Attacks on AES** Ali DOĞANAKSOY, Aslı DARBUKA, Dilek ÖZBERK, Neşe ÖZTOP, Fatih SULAK	**43 Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması** Şeref SAĞIROĞLU, Onur BEKTAŞ, Murat SOYSAL
09:40 - 10:00			**"Kayıtlı Elektronik Posta Sistemi Konusunda Araştırma, Geliştirme ve Uygulamalar Projesi"** Cafer CANBAY, Bilişim Uzmanı	**19 Algebraic Cryptanalysis of Reduced AES** Ameneh FARHADIAN, M.R. AREF	**48 IPv6 İkili Yığın Geçiş Yönteminde Uygulamaların Saldırı Altında Performans Analizi** Beyhan ÇALIŞKAN, Onur BEKTAŞ
10:00 - 10:20		10:00-10:45 TURKCELL **"Bugünden Yarına Mobil İmza"** Mehmet TURAN	**"Ulusal IPv6 Protokol Altyapısı Tasarımı ve Geçişi Projesi"** Ayşegül BOLAT, Bilişim Uzmanı	**40 A Survey of Related-Key Attacks on AES** Ali DOĞANAKSOY, Aslı DARBUKA, Dilek ÖZBERK, Neşe ÖZTOP, Fatih SULAK	**47 Kablosuz Algılayıcı Ağlarda Güven ve Zaman Tabanlı Solucan Deliği Tespit Algoritması** Suat ÖZDEMİR, Majid MEGHDADI, İnan GÜLER
10:20 - 10:40			**"Mobil Cihaz Kayıt Sisteminde e-imza Kullanımı"** Özgür ÖZTÜRK, Bilişim Uzmanı Yrd.	**16 Cryptanalysis of Strengthened Magenta** Orhun KARA	**41 Analysis of Attacks towards Turkish National Academic Network** Murat SOYSAL, Onur BEKTAŞ
10:40 - 11:00			**"Açık Anahtar Altyapısı Konusunda Araştırma, Geliştirme ve Uygulamalar Projesi"** K. Sacid SARIKAYA, Bilişim Uzmanı		**55 Pasif Ağ Verileri Üzerinden Düzensizlik Tespiti** Devrim SERAL, Beyhan ÇALIŞKAN
11:00 - 11:20	**ÇAY/KAHVE ARASI** TEA / COFFEE BREAK				
11:20 - 13:00	**Eğitim II** **KRİPTOGRAFİK ALGORİTMA ve MODÜLLERİN TEST, VALİDASYON ve SERTİFİKASYON SÜRECİ** Eğitmen: Ahmet Hasan KOLTUKSUZ İzmir Yüksek Teknoloji Enstitüsü	KURUMSAL SUNUMLAR	**Kamu Kurumları Özel Oturumu** Oturum Başkanı: Macit ÇOBANOĞLU Bilgi Güvenliği Derneği DK. Başkanı	**Oturum 9: BİLGİ GÜVENLİĞİ** Oturum Başkanı: Atilla ÖZGİT ODTÜ, Bilgisayar Mühendisliği Bölümü	**Oturum 10: GÜVENLİK ÇÖZÜM ÖNERİLERİ - 1** Oturum Başkanı: Ali YAZICI Atılım Üniversitesi, Bilgisayar Mühendisliği Bölümü
11:20 - 11:40		11:00-11:45 TÜRK TELE KOM	**"MEB ISO 27001 BGYS Sertifikası Alma Deneyimi"** Turan ŞIŞMAN, MEB/EĞİTEK BİM Daire Başkanı.	**39 CMS Tabanlı Kütüphane Kullanarak ETSI Uyumlu Elektronik İmza Modülü Geliştirmek** Hasan GÖLLE, Şeref SAĞIROĞLU	**30 Provable Electronic Marketplace Bidding Auction Protocol with Bid Privacy** Wenbo SHI, Injoo JANG, Hyeong Seon YOO
11:40 - 12:00			**"Kurumsal Uygulamalarda Bilgi Güvenliği"** Ömer ARIKAN, Cumhurbaşkanlığı Genel Sekreterliği,EBİS Daire Bşk.	**33 Policy Negotiation System Based on Privacy Preference** In Joo JANG, Wenbo SHI, Hyeong Seon YOO	**34 A Strong Two-Way Authentication Method for Low Cost Solutions** Gökhan DALKILIÇ, Hafize ÇAKIR, Mehmet ÖZCANHAN
12:00 - 12:20		12:00-12:45 TÜRKSAT	**Adalet Bakanlığı Projesi "Mobil Uygulamalarla Sağlanan Hukuki Koruma"** Hakim Muhammet POLAT	**21 Partially Opened Data and Its Security** Hidema TANAKA	**44 Çoklu Etmen Sistemlerinde Rol Tabanlı Erişim Denetimi İçin Bir Yaklaşım Önerisi** Fatih TEKBACAK, Oğuz DİKENELLİ, Tuğkan TUĞLULAR,
12:20 - 12:40			**"Akademik Ağ Güvenliği"** Serkan ORÇAN, TÜBİTAK/ULAKBİM Teknik Müdür Yrd.	**14 Project TWOVAULT - Secure and Selectively Deniable Data Storage** Markku-Juhani SAARINEN	**57 SCIP (Secure Communication Interoperability Protocol)'in IP Ağları Üzerinde Uygulaması** Orkun DİLLİ, Mehmet MERT, Murat KOYUNCU, Seday NAZLIBİLEK, Nursel AKÇAM
13:00 - 14:00	**ARA** BREAK				
14:00 - 15:40	**PANEL III** **Kurumsal Bilgi Güvenliği Nasıl Sağlanmalı?** **Panel Başkanı:** Mustafa ÜNVER, BTK/ BİM Daire Başkanı / Bilgi Güvenliği Derneği Yönetim Kurulu Üyesi Mehmet ALTINSOY, MEB/ EĞİTEK Genel Müdür Yardımcısı Ahmet KAPLAN, TÜRKSAT Genel Müdür Yardımcısı Eren ERSOY, Bilgi Teknolojileri ve İletişim Kurumu, Kurumsal Güvenlik Uzmanı Ahmet PEKEL, Merkez Bankası Bilişim Güvenliği ve Kalite Denetimi Müdürü Hayrullah KALE, Kurumsal Bilgi Yönetimi Müdürü, STM A.Ş.	KURUMSAL SUNUMLAR 14:00-15:00 KARAKOYA GROUP			
16:00 - 16:20	**ÇAY/KAHVE ARASI** TEA / COFFEE BREAK				

bilimsel program
scientific programme

2. gün
second day
26 Aralık December **2008**
Cuma Friday

	KEMAL KURDAŞ SALONU	A SALONU	B SALONU	C SALONU	D SALONU
16:20 - 18:00	**Eğitim III:** **KURUMSAL BİLGİ GÜVENLİĞİ** Eğitmen: Yılmaz VURAL, Bilgi Güvenliği Uzmanı, Bilgi Güvenliği Derneği, STM A.Ş.	KURUMSAL SUNUMLAR	**Özel Sektör Oturumu** Oturum Başkanı: Yüksel SAMAST Bilgi Güvenliği Derneği II. Başkanı	**Oturum 11: GÜVENLİK ÇÖZÜM ÖNERİLERİ - 2** Oturum Başkanı: Murat AŞKAR ODTÜ, Elektrik Elektronik Mühendisliği Bölümü	**Oturum 12 : BİLGİ GÜVENLİĞİ HUKUKU** Oturum Başkanı: Cumhur ŞAHİN Gazi Üniversitesi Rektör Yardımcısı
16:20 - 16:40			**"Savunma Sanayinde Güvenlik"** Hayrullah KALE Kurumsal Bilgi Yönetimi Müdürü Pınar UÇMAK Bilgi Güvenliği Yöneticisi, STM A.Ş.	15 **RFID Sistemlerinin İncelenmesi ve Mikroişlemci Üzerinde Güvenli Olacak Şekilde Gerçeklenmesi** Kaan BULUT, Berna ÖRS, İlker YAVUZ	10 **Uluslararası Ülke Güvenliğinde Hukuki ve Teknik Yaklaşım** Köksal ÖZENÇ, Mustafa ALKAN, Tayfun ACARER
16:40 - 17:00			**"Kritik Tesis ve Altyapıların Korunmasında Bilgi Güvenliği"** Dr. Tacettin KÖPRÜLÜ Havelsan A.Ş.	4 **Proposing a Wireless PKI Model Optimized for M-Commerce Applications** Fariborz Mousavi MADANİ, Iran BİMAR	31 **Dijital Hak Yönetimi ve Hukuksal Düzenlemeler** Caner AŞÇIOĞLU, Rüya ŞAMLI
17:00 - 17:20		17:00-18:00 Adobe **"Akıllı Belgeler ile Birlikte Çalışabilir E-Kurumlar"**	**BİLGİ GÜVENLİĞİ DERNEĞİ ÇALIŞMA GRUPLARI TOPLANTISI - I**	36 **Single Transferable Electronic Voting Protocol for Elections with Barriers** Okan YÜCEL, Nazife BAYKAL	12 **Bir Sanal Noter Uygulamasının Teknolojik ve Hukuki Gereksinimleri** Dursun AKÇEŞME, A.Çoşkun SÖNMEZ
17:20 - 17:40				54 **Eşler Arası Anonim Dosya Paylaşımı için Açık Anahtarlı Bir Kerberos Kimlik Denetimi Uygulaması** Tuğkan TUĞLULAR, Can MÜFTÜOĞLU, Özgür KAYA	
17:40 - 18:00				20 **An Intelligent and Automatic Eye Generation System from Only Fingerprints** Necla ÖZKAYA, Şeref SAĞIROĞLU	

3. gün
third day
27 Aralık December **2008**
Cumartesi Saturday

bilimsel program
scientific programme

	KEMAL KURDAŞ SALONU	A SALONU	B SALONU
09:30 - 11:00	**Eğitim IV:** **ÜLKE GÜVENLİĞİNDE BELGE GÜVENLİĞİ YÖNETİMİ** Eğitmen: Onur KARABULUT Karakaya Group	**Eğitim V:** **KİŞİSEL BİLGİ GÜVENLİĞİ** Eğitmen: Mehmet ÜNER Microsoft	
11:00 - 11:20	**ÇAY/KAHVE ARASI** TEA/COFFEE BREAK		
11:20 - 13:00	**PANEL IV** **Adli Bilişim Uygulamalarında Sorunlar ve Çözüm Önerileri** **Panel Başkanı:** Mehmet KÖKSAL, TBD Özgür ERALP, Ankara Barosu Gökhan AHİ, İstanbul Barosu Mehmet YÜCESOY, Bilişim Suçları Savcısı Cenk CEYLAN, Göktürk LTD. Ayhan ŞEHRİN, EBS Ltd., Bilgi Güvenliği Derneği	**Eğitim VI:** **MICROSOFT GÜVENLİK AİLESİ** Eğitmen: Mehmet ÜNER Microsoft	**BİLGİ GÜVENLİĞİ DERNEĞİ ÇALIŞMA GRUPLARI TOPLANTISI - II**
13:00 - 13:20	**KAPANIŞ** CLOSING CEREMONY		