

**Press Contacts:**

**MediaCrypt/US**  
Judith Jameson  
+1 (781) 862-1451  
jamesongroup@rcn.com

**MediaCrypt/Europe & Asia**  
André Simmen  
+41 (32) 622 9552  
simmen.solothurn@bluewin.ch

**EPFL**  
Nicolas Henchoz  
+41 (21) 693 5073  
nicolas.henchoz@epfl.ch

Pascal Junod  
+41 (21) 693 7617, +41 (78) 896 6794  
pascal.junod@epfl.ch

## **MEDIACRYPT & EPFL ANNOUNCE NEXT-GENERATION ENCRYPTION ALGORITHM RESEARCH PROJECT “FOX”**

### **For Content And Copyright Protection Market/ In Video And Audio**

**-- Based on Customer Requirements:  
Increased Security, Improved Performance & Flexibility --**

**Geneva, Switzerland – ITU Telecom World – Hall 4/Booth # 4241-012/Swiss Pavilion --  
October 10, 2003** – MediaCrypt (of Zurich, Switzerland) and EPFL (the Swiss Federal Institute of Technology, Lausanne) have today presented their encryption research project named ‘FOX’, targeting the media distribution industry. FOX consists of a new block cipher algorithm for symmetric encryption and a new key management system. FOX comes to the public for review and testing, following the footsteps of the successful IDEA™, MediaCrypt’s Ascom’s encryption algorithm that has remained strong and reliable for over 10 years. MediaCrypt markets IDEA exclusively, worldwide. FOX incorporates protection against the latest mathematical attack methods.

The scientific part of the FOX project was conducted in the Security and Cryptography Laboratory of EPFL (LASEC), and was managed by Professor Serge Vaudenay and Pascal Junod. This project is also part of Junod’s Ph.D. thesis, which will be formally submitted in 2004. Once numerous algorithm skeletons were created and carefully studied, the best one was chosen and sent out to two independent experts in the cryptography arena. After some fine-tuning, the final algorithm was put through some rigorous implementation experiments and a request for two patents was submitted.

**-- more --**

## **MediaCrypt and EPFL Announce New Encryption Research Project – 2 of 2**

Pascal Junod, of EPFL FOX project, noted, “Nowadays, a modern block cipher must be able to be implemented on various platforms, as hardware implementation or as software implementation, ranging from low-cost smart cards to modern 32- and 64-bit processors. FOX was carefully designed in order to meet the highest standards in terms of speed and flexibility while keeping a very high security level.

“What distinguishes the FOX algorithm from others is that we took our time designing it carefully, followed by obtaining two independent evaluations. FOX was not designed in a hurry, just to meet some standardization process deadline like most of its competitors,” stated Serge Vaudenay of EPFL. “We believe that our design process and review by outside experts is what makes FOX exempt of security weakness and that it will successfully pass through the public evaluation by academic research.”

“The area of secret-key cryptography is rather elusive – there is no way, using current state-of-the-art process, to mathematically prove the security of an encryption algorithm. This is why we rely on expertise and evaluation of academic research and in this case, the talents of the EPFL design team,” said Richard Straub, CEO of MediaCrypt. “Professor Vaudenay and Pascal Junod are worldwide recognized crypto experts. Their knowledge and expertise, combined with direct input from our current IDEA customers, allowed for a very fast, tight and truly flexible algorithm to evolve.”

**Availability:** Test Licensing upon Request and Approval. Contact MediaCrypt at [info@mediacrypt.com](mailto:info@mediacrypt.com) for further information.

#####

### **About EPFL**

Located in Lausanne, Switzerland, the EPFL is the host of large national centers of competence and research, particularly in communication systems and photonics. It collaborates on several hundred international projects. Its mission is to develop the results of research work, and, helped by its science park, it produces an average of one new company per month. The EPFL has 6,000 students, 230 professors, and 3,220 scientific researchers, technicians, and support personnel in 12 fields of teaching and research. For more information, please see [www.epfl.ch](http://www.epfl.ch).

### **About MediaCrypt AG**

MediaCrypt develops and licenses encryption algorithm software, based on Ascom’s International Data Encryption Algorithm (IDEA). IDEA has been widely recognized and accepted as a vital business component in highly secure encryption systems, since its debut in 1991. The company services hundreds of customer applications and millions of users worldwide. Headquartered in Zurich, Switzerland, MediaCrypt targets markets that are involved in the convergence of Internet, Multimedia, Entertainment and Wireless Communications. Primary customer segmentations include content and copyright protection solutions like Conditional Access and Digital Rights Management (DRM), as well as component builders/manufacturers for trusted devices for the digital home. The company is owned equally by its two Swiss founders, Ascom (ASCN: SWX) and the Kudelski Group (KUD: SWX). For more information, please see [www.mediacrypt.com](http://www.mediacrypt.com).

Note to Editors: MediaCrypt is a trademark of MediaCrypt AG. IDEA is a trademark of Ascom.