INTERPOL

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

INTERPOL & GLACY+ Technical Webinar: Crypto for Criminal Justice Authorities

1-10 December 2020

Date and hour	01/12/2020, 13h00 UTC Webinar 1 (Hash and Crypto Essentials)
	03/12/2020, 13h00 UTC Webinar 2 (Symmetric cryptography)
	07/12/2020, 13h00 UTC Webinar 3 (Asymmetric cryptography)
	08/12/2020, 13h00 UTC Webinar 4 (Trust in Internet - digital certificates)
	10/12/2020, 13h00 UTC Webinar5 (Darknet and Cryptocurrencies)
Speakers	Alvaro ORTIGOSA, Universidad Autónoma de Madrid Carlos PIMENTEL, Portuguese Guarda Naciona Republicana Belhassen ZOUARI, University of Carthage, Carthage Mark van STAALDUINEN, CFLW Cyber Strategies
Expected duration	Each webinar will take maximum 90' minutes for presentations and discussions
Facilitator	Dong Uk KIM, INTERPOL
Objectives	Webinar 1. To start the first of the series, we aim to discuss the characteristics of the hash function, and why it is useful in information security as well as in electronic evidence. We will continue discuss on the basic concepts of ancient cryptography and cryptanalysis as a primer to the modern cryptography to be followed in coming webinars.

	Webinar 2. Modern cryptography came with automation. In the webinar we will visit how the information is kept confidential using the cryptographic algorithms and security of secret keys. We will then address the difficult question of how two communication parties can share a common secret key, without meeting each other before the communication. Webinar 3. The number of keys exponentially becomes too many as newer members participate in the Internet. In this webinar, we discuss on how the reusable keys are developed, and how the public-key encryption can provide the new capability of entity verification. Webinar 4. One of the applications of cryptography is the green padlock on the address bars of some modern web browsers. It gives the users the sense of security. In this webinar we discuss how the HTTPS works and how much trust we can give to these padlocks. Webinar 5. Hash and public key encryption enable the cryptocurrencies and dark net. We will briefly go through what cryptographic technologies are used to make these applications possible.
Expected outcomes	The first part of the webinars (1,2 and 3) aim to provide knowledge and conceptual understanding of cryptography necessary to conduct daily duties for the criminal justice authority officials. After the webinars, the participants will discover: – Characteristics and capabilities of good cryptographic hash function – How passwords are stored and stolen – Conceptual orientation of algorithms in the context of ancient cryptography – Modern block symmetric cryptography and the capabilities it provides – How two parties can share secret key in the presence of eavesdropper (internet) – Why reusable public keys are useful for network with large participants – How the concept of public key was realized (example of RSA). – Non-repudiation capabilities of public key encryption In the webinar 4 and 5, the participants will have chance to discuss with the speakers on more applied real-life examples of cryptography-induced trust. – How the public key encryption was applied to become the pad-lock icon (https) in the address bar of the web-browser. – How much trust can we give to the certificates, and why (HTTPs: who verifies the entity, and how?)

	– How hashing and public key encryption applied in Blockchain and cryptocurrency transactions in Bitcoin.
Participants	The webinars are open for the officials working in the criminal justice authorities.
Background	As the use of and reliance on information technology becomes more and more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and in sophistication, and criminal justice authorities are called to face an ever-increasing number of challenges in order to ensure efficient investigation and successful prosecution of related crimes. Many countries have undertaken efforts in recent years to establish specialized cybercrime units at the level of police authorities, as well as units responsible for digital forensics. Cryptography is the one of the core technological enabler of the information technology being so widely received by the public. Without it, the little trust in the Internet would have prevented the network to grow so large. However, the knowledge of cryptography has not been covered enough in the context of the law enforcement training. In the framework of GLACY+ project, this training topic was first piloted in the first responder training hosted by the European Cybercrime Training and Education Group (ECTEG) and INTERPOL in September 2020 as part of the E-First package.
Relevant resources	Council of Europe, The Budapest Convention and related standards Council of Europe, Standard Operating Procedures for the collection, analysis and presentation of electronic evidence (upon request) Council of Europe, Electronic Evidence Guide (upon request) Council of Europe, Digital Forensic Lab Guide
C-PROC related activities	