A Tutorial of White-Box Cryptography Chapter 1 Overview

Zheng Gong[1,2]
cis.gong@gmail.com

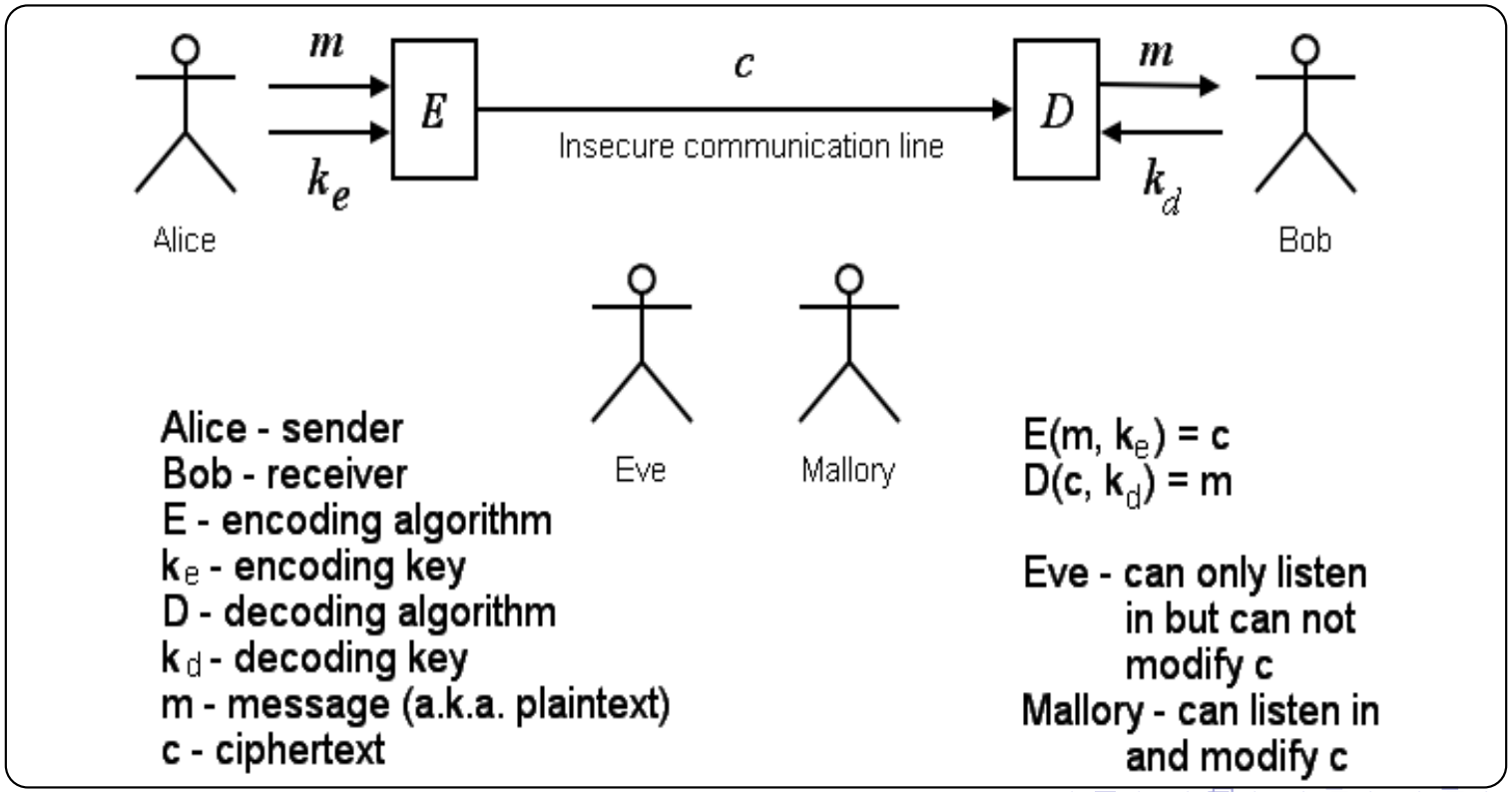
[1]School of Computer Science, South China Normal University
[2]Mobile Applications And Security Engineering Center of Guangdong Province

August 14, 2018

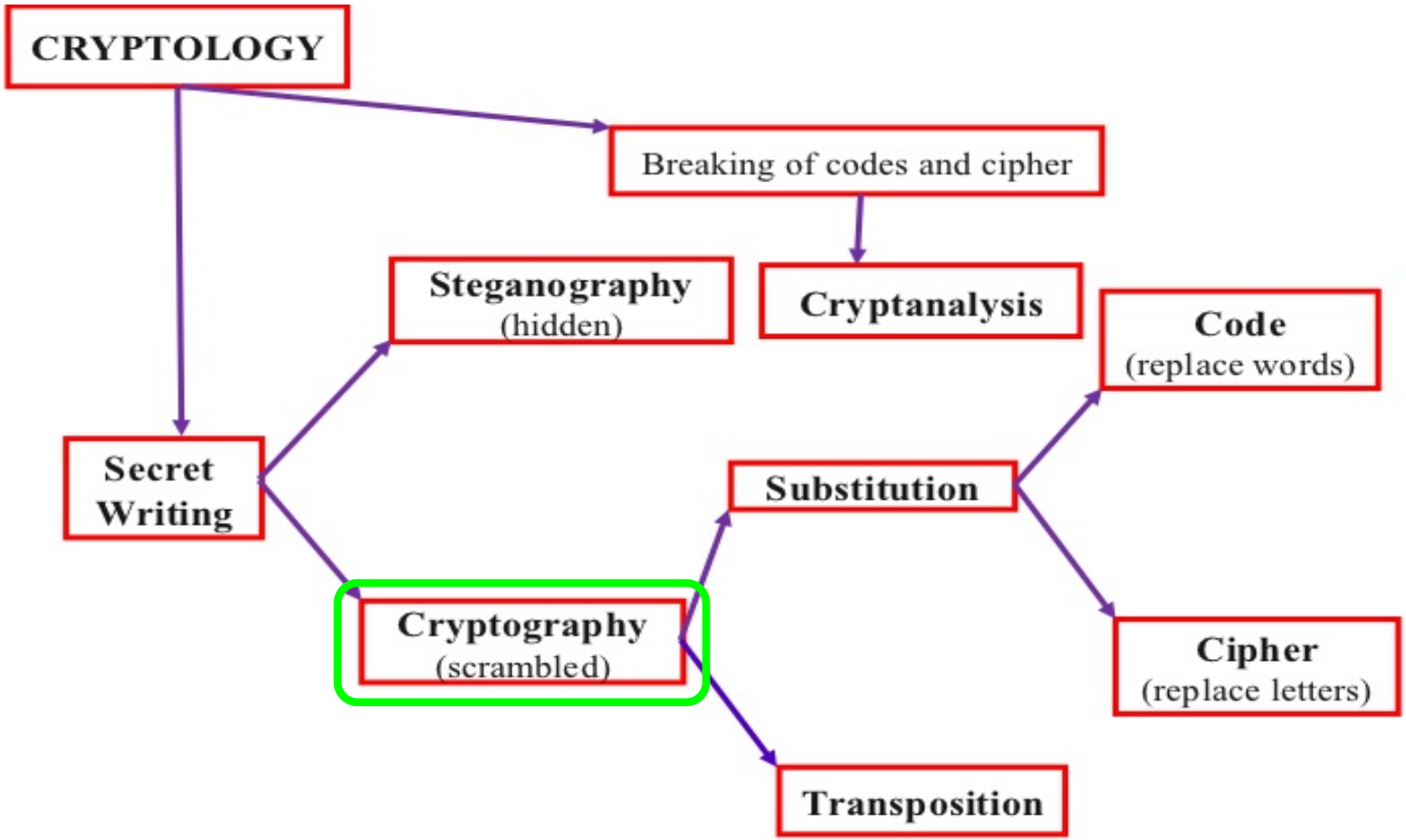
What is cryptology?

"Cryptology is about communication in the presence of adversaries or potential adversaries"

- R. Rivest



What is cryptography?

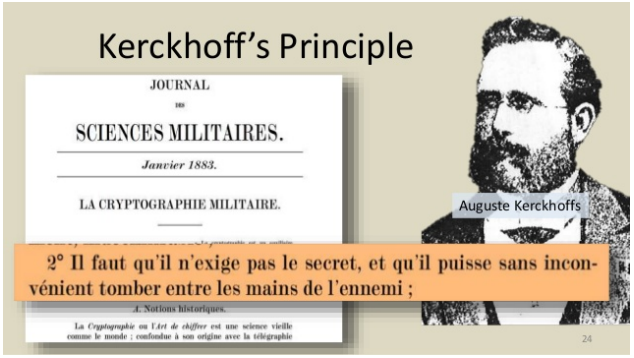


What we need for cryptography?

- Confidentiality: not just mean en/decryption, it imposes allow authorized people access privileged data
- Integrity: not just mean signature, it includes how to prove the originality and the tractability of the data
- Applicability: The cryptosystems must be practical

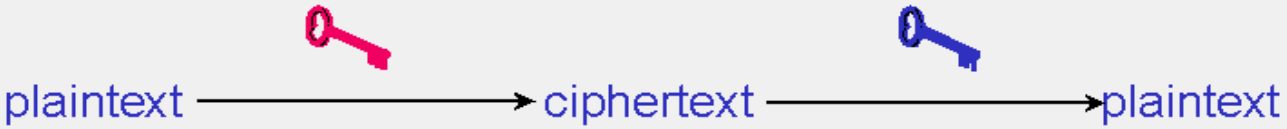
Kerckhoffs principle

- Do not rely on keeping an algorithm secret
- Publish an algorithm but keep the key secretly
- Have some mathematical foundation for the belief that it will be hard to extract the key



Different key types in cryptosystems

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.



B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Threat model of secret key (1)

- There are three combinations in the mobile application threat model.
  - Benign host, Malicious client (APPs?)
  - Malicious host, Malicious client (Cloud service?)
  - Benign host, Benign client (VPN?)
- In most of mobile applications, hosts are assumed to be benign whilst client might be malicious or controlled by adversary.

Threat model of secret key (2)

- Black-box model: the adversary cannot intrude/alternate/observe the inside of the cryptosystem;
- Grey-box model: the adversary can partially intrude/alternate/observe the inside of the cryptosystem;
- White-box model: the adversary can fully intrude/alternate/observe the inside of the cryptosystem;

Applications of black/grey-model-secure products

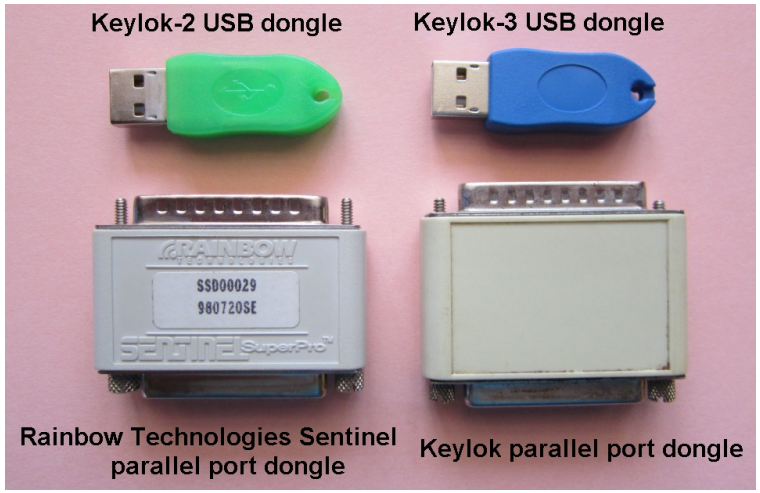
- A typical example is the maturing of USB keys
- The various manufactories and vendors provide different solutions to make RSA/ECC onboard (which also deliberately design to resist grey-box attackers).
- Eventually it works like a secure black box (and still evolving)

USB Key型号	外形特征
捷德	
海泰	
飞天	
文鼎创	

Hardware-aided software security

In practice, many kinds of hardware are used to protect software security

- Environment validation: TPMs
- Authenticity: USB keys, TPMs
- Functionality: SE, Crypto ICs, Software USB doggles



Why we need white-box crypto?

- Although hardware-protected black/grey-box solutions are matured in the last decade, software solutions are still useful in many areas.
- To the best of my knowledge, the white-box crypto (which includes symmetric/asymmetric-key cryptosystems) is pivotal for the following practical issues.
  - Hardware protection is costly (price)
  - Hardware solution is incompatible (interoperability)
  - Extreme system security protection (key obfuscation)
  - Algorithm implementation flexibility and complexity (Complex functionality requirements)

“counter-examples” on the hardware interoperability

Threat in software solutions

Although software solutions enjoy the interoperability and flexibility, the security problems rise.

- emulation
- run step-by-step in a debugger
- disassemble/decompile

One usually refers to the above attacks as a *white-box* adversary.

Informal definitions of white-box crypto (1)

Informally I have the following concerns about white-box crypto:

- From the view of crypto key security, it implies
  - secret key protection: adversary cannot extract secret key from software (no matter whether running or not)
  - key distribution mechanism: only designated user/server can generate the white-box version secret key (quite close to public-key crypto, but not exactly the same)

Informal definitions of white-box crypto (2)

- From the view of software developer, it implies
  - cryptographic obfuscation: the algorithm is public, but only the secret key is obfuscated
  - code/space/time hardness: the time/memory/space complexities will increased (heavily)
  - Function abstraction: After white-box implementation, a function's inner functionality is no longer publicly verifiable

Differences between software obfuscation and white-box crypto

Software obfuscation and white-box crypto can operate together to achieve concrete security, while they have different purposes:

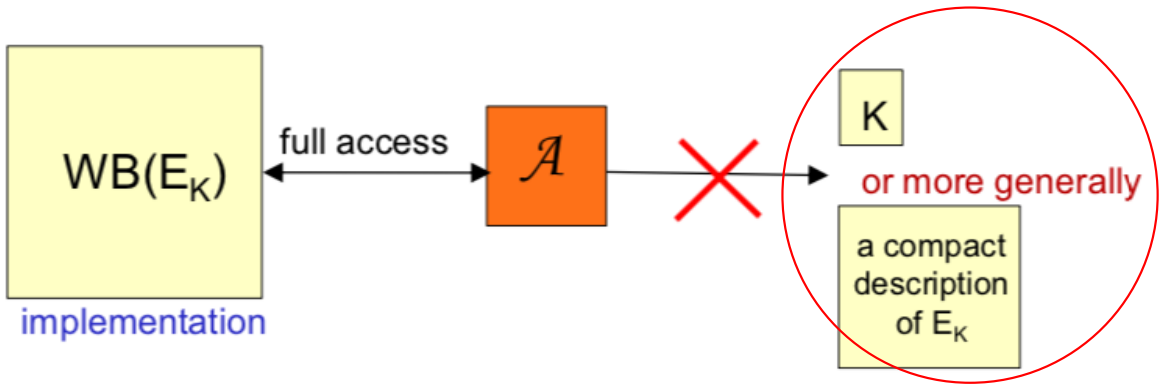
- Software obfuscation does not look for theoretically secure levels of white-box crypto, it should be feasible for practice
- White-box crypto must be secure either in theory or computational complexity
- Software obfuscation merely seeks to increase the reverse-engineering costs in a sufficiently discouraging manner for adversary

White-box crypto working range

- To resist adversary, a software should be secure against:
  - Static analysis: from binary code to extract information
  - Dynamic analysis: from memory to extract information
  - Code lift: change the execution order/function, which breaks the integrity of software
- For white-box crypto, we mainly focus on
  - functionality is executed as designed
  - key is not leaked

Basic security definitions for white-box crypto (1)

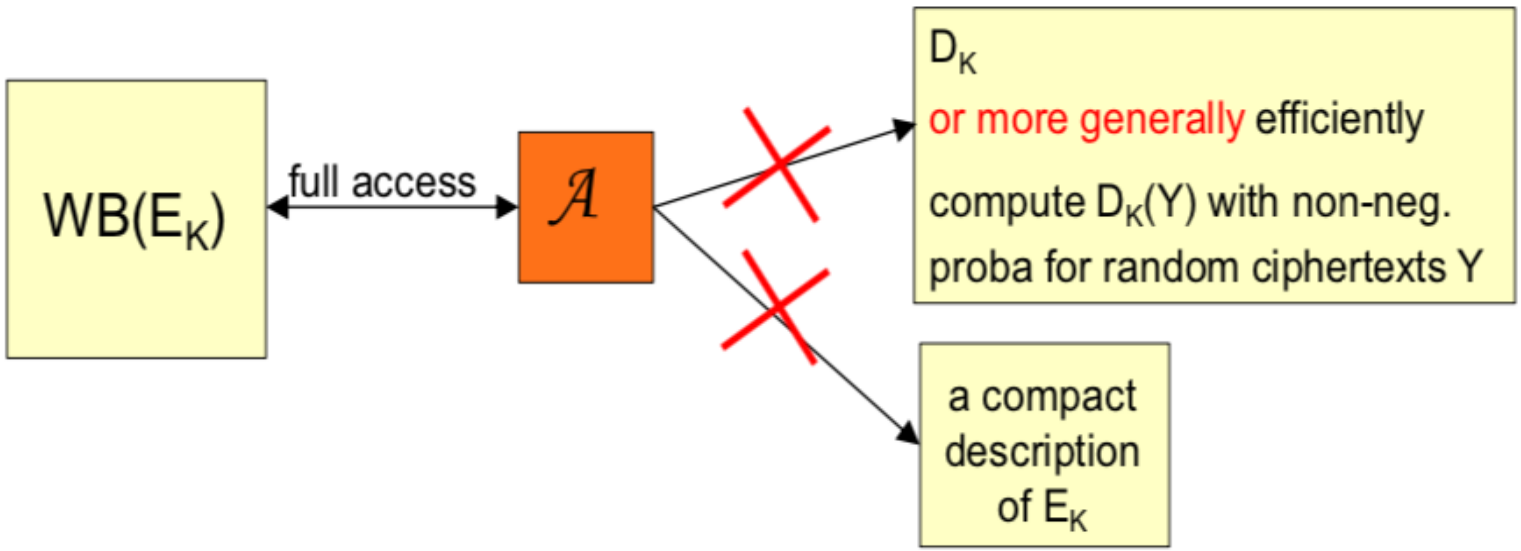
- In SAC 2002, the security notions have been informally described for white-box cryptography by Chow *et al.*. First the key recovery problem is informally defined by the weak white-box security



informal definition: (T, S)-incompressible implementation of E_K.
an adversary with full access to WB(E_K) must be unable to derive
an equivalent* representation of E_K of size lower than S in time T. **

Basic security definitions for white-box crypto(2)

- For more general security, the strong white-box security has been defined by Chow et al.



- Software security is significant for protecting applications in practice
- Software obfuscation and white-box cryptography are different fruits on same tree
- Applications have various requirements on white-box crypto

Thanks for your attentions!