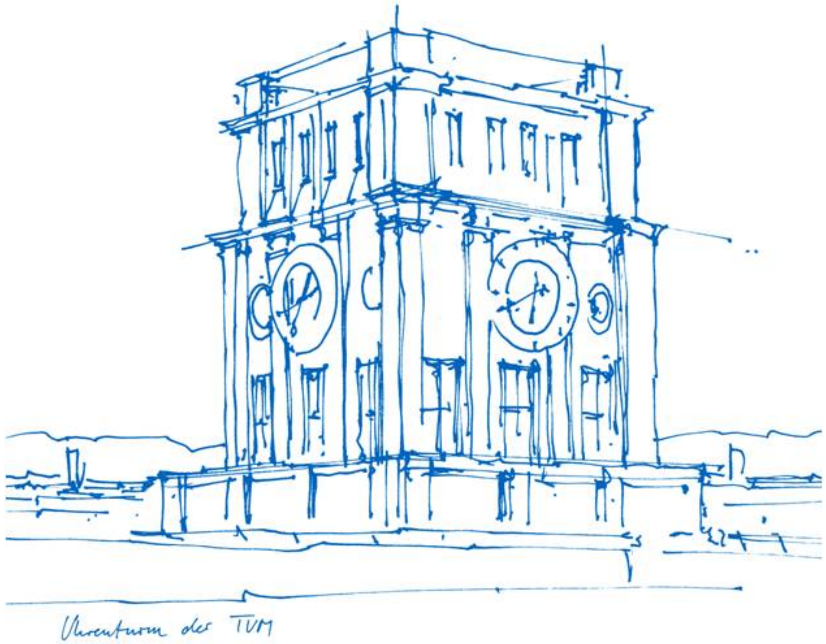
07 Cryptography 1

Heiko Niedermayer,

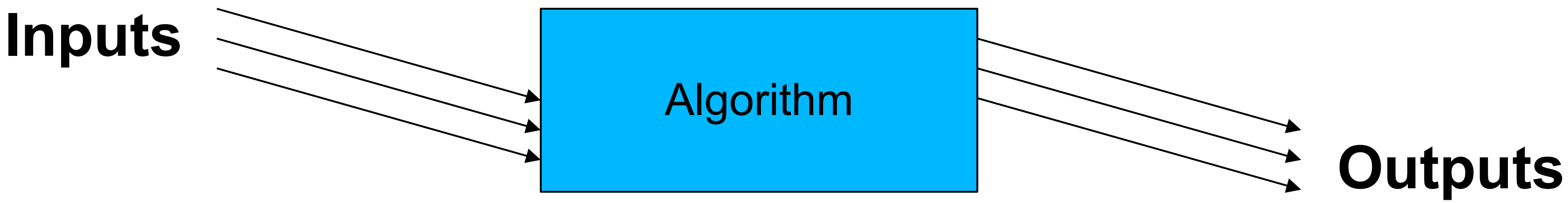
Georg Carle



Overview

- Overview of Cryptographic Algorithms
- Achieving a Security Goal
- Security Models and Security of Crypto Schemes
- Eavesdropping Experiment
- Chosen-Plaintext Attack

Overview of cryptographic algorithms



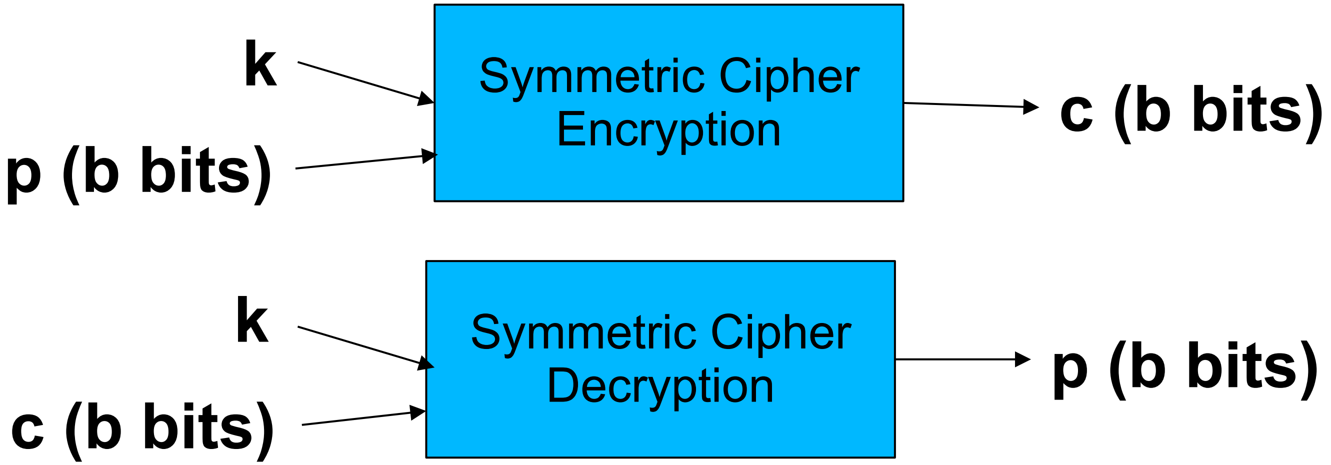
Cryptography provides a variety of algorithms that it uses as building blocks for generating schemes and protocols that achieve a given set of security goals.

- Symmetric Block Cipher
- Cryptographic Hash Function
- Asymmetric Cipher (Public Key Cryptography)
- …

Example

- AES-CTR
  - AES is a symmetric cipher
  - Counter Mode (CTR) is a method to encrypt plaintext with a symmetric cipher to achieve confidentiality
  - Inputs: key k, plaintext p
  - Outputs: ciphertext c
  - Requirements: p and k need to remain confidential
- Key Derivation Functions (KDFs)
  - Problem: you have k bits of entropy / key, needed m bits for keys
  - Input: k1 with k bits
  - Output: k2 with m bits
  - Requirements: entropy of k2 not lower than entropy of k1
  - KDFs can be built from cryptographic hash functions, symmetric ciphers, …

Symmetric Block Cipher

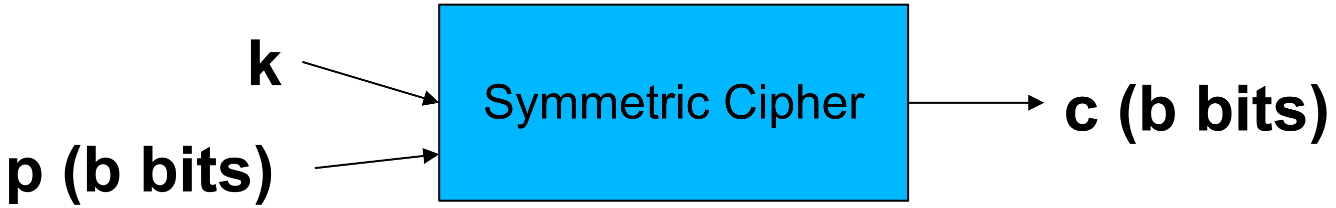


- Block cipher with block length b
- Typical lengths for block and key: 64 bits, 128 bits, 256 bits
- Already known from section on Symmetric Cryptography
  - Note: There are also symmetric stream ciphers. Internally, they may have the concept of blocks as well.

Symmetric Block Cipher

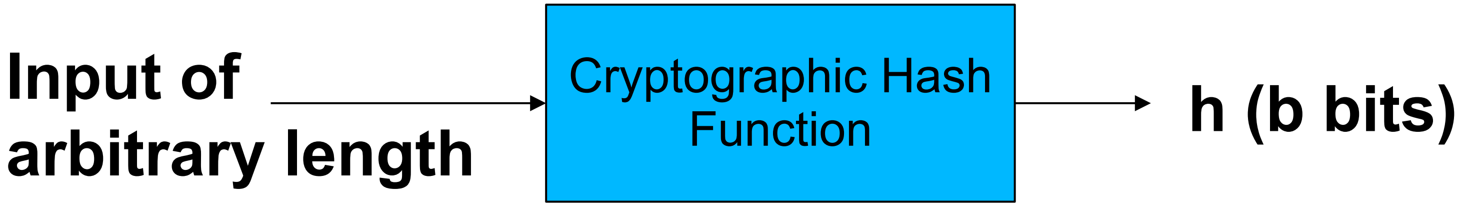
- Operation
  - Needs to contain non-linear element
  - Concept of Confusion
    - Confusion = 0s and 1s can generate output with completely different statistics with respect to 0s and 1s
    - 00000000 can become 11111111, most likely something like 10110100
  - Concept of Diffusion
    - Diffusion = any bit influences bits at other positions, goal: influences all bits
  - Typically, the ciphers repeat a similar set of operations (e.g. for confusion and diffusion) over multiple rounds with round-specific inputs.

Symmetric Block Cipher



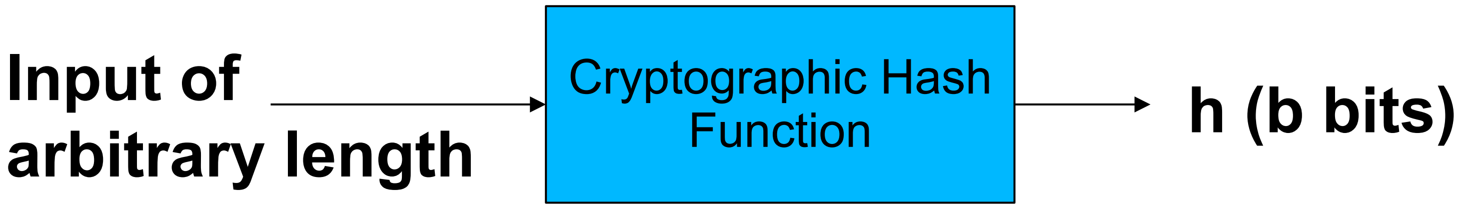
- Evaluation
  - Application of the block cipher should neither leak the key k nor the plaintext p.
  - Brute Force attack:
    - Try all possible keys, e.g. given plaintext and ciphertext pair
    - Key k with n bits, $O(2^{n-1})$ average case complexity
  - Security of cipher:
    - If best attack on cipher is much better than brute force or if it is computationally feasible, then considered broken.
    - 2^a complexity => a “bits of security”

Cryptographic Hash Functions



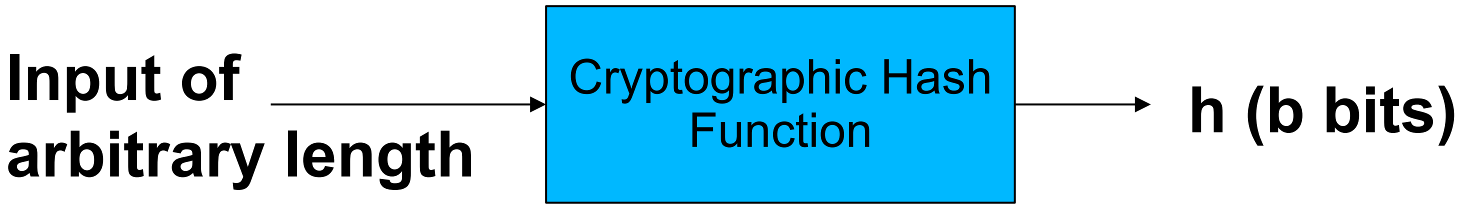
- We will have a chapter on cryptographic hash functions.
- Cryptographic hash functions are hash functions with special properties needed for security, e.g. (not complete list)
  - 1st Pre-Image Resistance: Make it hard to find an input m that produces a given output h
  - Collision Resistance: Make it hard to find two pairs of input m1, m2 that produce the same output (collision)

Cryptographic Hash Functions



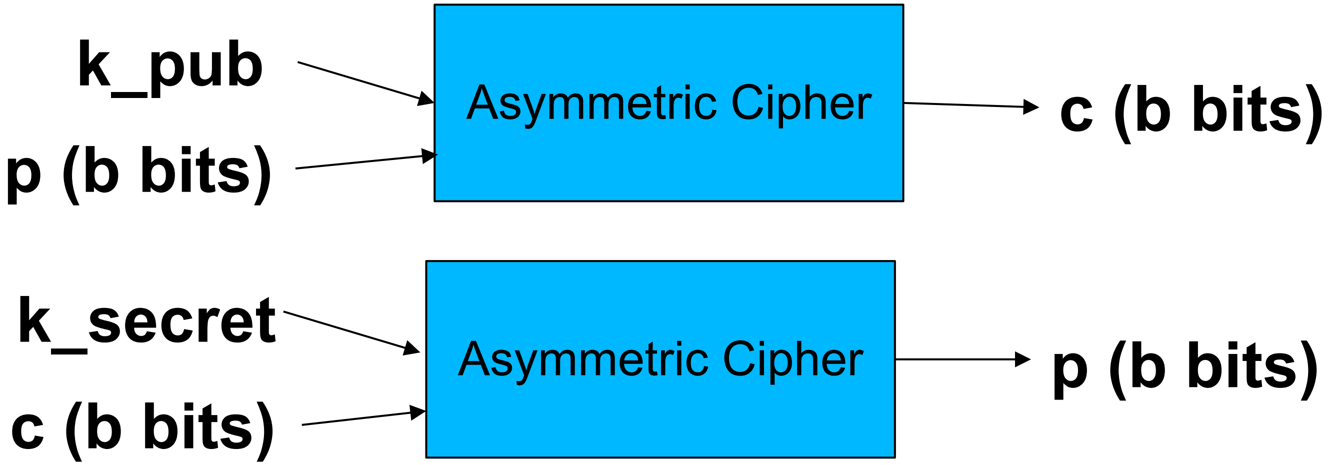
- Operation:
  - Similar to symmetric block ciphers
  - In addition, they need a way to include an arbitrary number of input blocks.
    - e.g. taking the last block of AES-CBC and make key pre-defined would be a cryptographic hash function
    - Traditional hash functions follow Merkle-Damgard constructions
    - Modern hash functions like SHA3 follow other constructions and have finishing functions after processing the last block

Cryptographic Hash Functions



- Evaluation:
  - Similar to symmetric block ciphers
  - Due to Birthday Paradox, only half of the bitlength contributes to collision resistance.
    - “160 bit hash function -> 80 bits of security”
    - Collisions can be found for perfect hash function with n bits output with $O\left(2^{n/2}\right)$

Public Key Ciphers



- We will have a chapter on asymmetric cryptography with more details.
- Each entity has public k_pub and secret key k_secret (also called private key)
- Other entities use the public key k_pub_A of A in interactions with A. A uses its secret key k_secret_A.

Public Key Ciphers

- Operation
  - Asymmetric ciphers are usually based on mathematical problems that are computationally hard
    - E.g. Factorization (RSA), Discrete Logarithm (ECC, Diffie-Hellman)
    - Most of these problems have efficient quantum algorithms. Thus, these ciphers are not quantum-secure.
- Evaluation
  - Attack the mathematical problem
  - Find weak cases
    - Hard problems are not necessarily hard in all cases. Weak parameters, weak mathematical groups are typical issues faces in asymmetric ciphers.

Achieving a security goal

- Symmetric Cryptography
- Goal: Confidentiality

- From the chapter on symmetric cryptography we already know
  - that simply applying the block cipher is not secure (ECB mode)!
  - that CBC or Counter mode provide security.
- How do we know that?
  - Traditionally, schemes were developed and security and insecurity depended on the best attacks found against the method.

Achieving a security goal – security models

- Modern cryptography tries to model the situation of achieving the security goal in a given setting more formally.
- Formal model
  - Needs precise and explicit definition of method and assumptions
  - Allows for mathematical proofs
  - Provides better understanding of properties needed
- Limitation
  - Model != Reality
  - Attacks may still exist, in particular where model assumptions clash with reality.

A model for confidentiality / Symmetric Cryptography

Notation:

$A \leftarrow B$ non-deterministic assignment, can contain some form of randomness

$A \coloneqq B$ deterministic assignment (no randomness)

$A = B$ comparison

A model for confidentiality / Symmetric Cryptography

Symmetric encryption scheme

$k \leftarrow Gen(1^n)$ # *random key is generated and known to the legitimate communication parnters*

$c \leftarrow Enc_k(m)$, $m \in \{0,1\}^*$

$m \leftarrow Dec_k(c)$

Such an encrpytion scheme is considered secure if it succeeds in a theoretical attack game using a chosen-plaintext attack.

In the game, the challenger $\mathcal{C}$ uses the scheme and adversary $\mathcal{A}$ tries to overcome the scheme.

Eavesdropping Experiment

Challenger $\mathcal{C}$ | Adversary $\mathcal{A}$

$k \leftarrow Gen(1^n)$ | $input\ 1^n$

m_0, m_1 of equal size selected by adversary

$\leftarrow m_0, m_1$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc_k(m_{\boldsymbol{b}})$

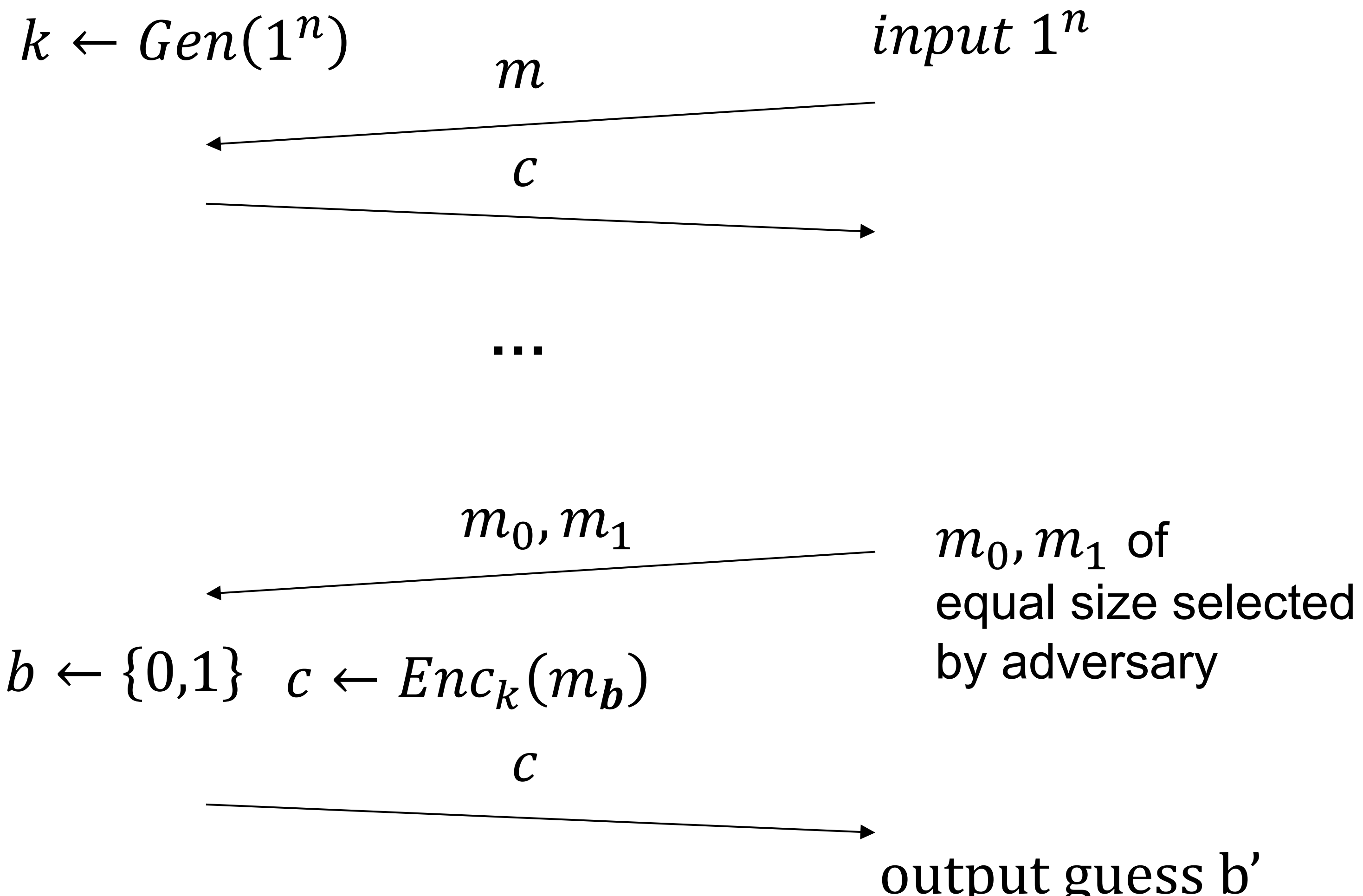
$c \rightarrow$

output guess b’

Adversary $\mathcal{A}$ succeeds if and only if b=b’

Eavesdropping Experiment – Chosen Plaintext Attack

In order to prepare for the game, the adversary is now allowed to utilize information from additional chosen plaintexts. It is allowed a polynomial time chosen plaintext attack.



Eavesdropping Experiment – Discussion

If the adversary simply guesses, 50 % chance that it will be correct, 50 % that the guess is incorrect. Thus, we cannot expect it to lose the game all the time.

- Enc is secure under Chosen-Plaintext attack (CPA)
  - if this polynomial time-bound adversary is not achieving a success rate above 0.5 + negligible
- This means that the adversary is not able to gain significant information from observing many ciphertexts and plaintext-ciphertext pairs.

- Question: Can the Dolev-Yao attacker do more to break the scheme than the adversary here?

Applying the model

Why is ECB not secure under the model?

- ECB is deterministic cipher scheme
- Identical blocks in plaintext are identical blocks in ciphertext
- The adversary just has to mark m_0 and m_1 with identical plaintext pairs in different positions.
- b=0 if identical ciphertext blocks in positions as in plaintext m_0, else $\mathrm{b} = 1$

Why is Counter Mode (CTR) secure under the model?

- CTR is non-deterministic, random initialization vector
- Be careful, counter value must not repeat

Deterministic vs Non-deterministic crypto schemes

- Cryptographic algorithms are deterministic algorithms
- Naively using them leads to deterministic crypto schemes which are not secure under CPA.
- However, deterministic encryption schemes have special use cases where they can make sense, but typically not in the security of network communication!
- When generating a crypto scheme to realize a security property, we usually need to generate a non-deterministic scheme.

References

[KL15] Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, 2nd edition, CRC Press, 2015