# Introduction to Modern Cryptography Summary

**WS20/21**

Valentin Knappich

January 21, 2021

## Contents

**1 Symmetric encryption** **2**
1.1 Scenario 1 . . . . . . . . . . 2
1.1.1 Cryptosystems . . . . . . . . . . 2
1.1.2 Vernam system . . . . . . . . . . 2
1.1.3 Perfect Secrecy . . . . . . . . . . 2
1.2 Scenario 2 . . . . . . . . . . 3
1.2.1 Vernam in Scenario 2 . . . . . . . . . . 3
1.2.2 Substitution Cryptosystem . . . . . . . . . . 3
1.2.3 l-Block Cipher . . . . . . . . . . 4
1.2.4 Substitution-Permutation Cryptosystem (SPCS) . . . . . . . . . . 4

# 1 Symmetric encryption

**Kerkhoffs Principle**: The security of a system should only depend on whether the actual key is secret, not on the system itself. The whole system is assumed to be public. No “Security by obscurity”.

## 1.1 Scenario 1

**One message with constant length**

### 1.1.1 Cryptosystems

A cryptosystem is a tuple $S = (X, K, Y, e, d)$ with

- X: set of plaintexts
- K: finite set of keys
- Y: set of ciphertexts
- e: encryption function
- d: decryption function

Perfect correctness: $d(e(x, k), k) \forall x \in X, k \in K$

No unnecessary ciphertexts: $Y = \{e(x, k) | x \in X, k \in K\}$

### 1.1.2 Vernam system

The Vernam cryptosystem of length $l$ is defined as $(\{0, 1\}^l, \{0, 1\}^l, \{0, 1\}^l, e, d)$ where

$e(x, k) = x \oplus k$ and $d(y, k) = y \oplus k$.

A vernam system of length $l > 0$ provides perfect secrecy for every uniform $P_K$. It is the perfect system for Scenario 1.

### 1.1.3 Perfect Secrecy

A cryptosystem with key distribution $V = S[P_k]$ provides perfect secrecy if for all plaintext distributions $P_X$, the probability of every plaintext remains the same, i.e.:

$$P(x) = P(x|y) \quad \forall x \in X, y \in Y, P(y) > 0$$

**Example Proof**:

We need to show the criteria above for all plaintext distributions $P_X$. Therefore we use variable probabilities for the plaintexts $P_X(a) = p, P_X(b) = 1 - p$ (for 2 plaintexts, else $p_1, ..., p_n$).

| $K \backslash X$ | | a | b |
|---|---|---|---|
| $\frac{1}{2}$ | $k_0$ | $A$ | $B$ |
| $\frac{1}{2}$ | $k_1$ | $B$ | $A$ |

$$P(a|A) = \frac{P(a,A)}{P(A)} \quad = \frac{\frac{1}{2} * p}{\frac{1}{2} * p + \frac{1}{2} * (1-p)} = p = P(a) \tag{1}$$

$$P(a|B) = \frac{P(a,B)}{P(B)} \quad = \frac{\frac{1}{2} * p}{\frac{1}{2} * p + \frac{1}{2} * (1-p)} = p = P(a) \tag{2}$$

$$P(b|A) = \frac{P(b,A)}{P(A)} \quad = \frac{\frac{1}{2} * (1-p)}{\frac{1}{2} * (1-p) + \frac{1}{2} * p} = 1 - p = P(b) \tag{3}$$

$$P(b|B) = \frac{P(b,B)}{P(B)} \quad = \frac{\frac{1}{2} * (1-p)}{\frac{1}{2} * (1-p) + \frac{1}{2} * p} = 1 - p = P(b) \tag{4}$$

**Theorem**:

Let $S = (X, K, Y, e, d)$ be a cryptosystem providing perfect secrecy, then it holds $|K| \geq |Y| \geq |X|$.

**Shannons Theorem**:

Let $V = S[P__k] be a cryptosystem with key distribution $P_K$ and $|K| = |Y| = |X|$. The system provides perfect secrecy if and only if

1. $P_K$ is a uniform distribution
2. $\forall x \in X, y \in Y \exists k \in K with e(x,k) = y$ (There must be a key for every plaintext/ciphertext pair)

## 1.2 Scenario 2

**Multiple messages with constant length, no repetition**

### 1.2.1 Vernam in Scenario 2

Vernam is not a secure cryptosystem anymore, since from 2 ciphertexts, Eve can learn non-trivial information about the plaintexts:

$$y_0 \oplus y_1 = x_0 \oplus k \oplus x_1 \oplus k = x_0 \oplus x_1$$

Also with 1 plaintext-ciphertext pair (CPA), the key can be calculated as $k = x \oplus y$.

### 1.2.2 Substitution Cryptosystem

Let $X$ be a non-empty finite set. A substitution cryptosystem over X is a tuple $(X, P_X, X, e, d)$ where $P_X$ is the set of all permutations of $X$.

$$e(x, \pi) = \pi(x) \quad d(y, \pi) = \pi^{-1}(y) \quad \forall x, y \in X, \pi \in P_X$$

Substitution cryptosystems provide “perfect security” in scenario 2, BUT they are impractical because the permutation table ($\pi$) has a size of $2^l * l$.

Therefore, we need a weaker security definition that takes into account, that attackers are resource bound.

### 1.2.3 l-Block Cipher

Let $l : \mathbb{N} \to \mathbb{N}$ be a polynomial. An l-block cipher $B$ is a cryptosystem of the form

$$\left(\{0,1\}^{l(\eta)}_{\eta\in\mathbb{N}},\ Gen(1^\eta),\ \{0,1\}^{l(\eta)}_{\eta\in\mathbb{N}},\ E,\ D\right)$$

or simplified:

$$\left(\{0,1\}^{l},\ Gen(1^\eta),\ \{0,1\}^{l},\ E,\ D\right)$$

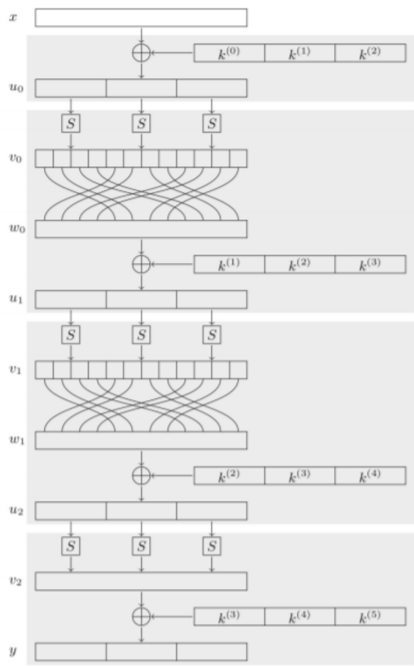
### 1.2.4 Substitution-Permutation Cryptosystem (SPCS)

**Notation**:

- plaintexts are split into $m$ words with length $n$ with $l = m * n$, $x^{(i)}$ denotes the $i$'th word
- $[r] = \{0, 1, ..., r-1\}$
- $\beta \in P_{[l]}$, then $x^\beta(i) = x(\beta(i))$

**General Principle**: Over $r$ rounds, (round) key additions, word substitutions and bit permutations are applied, including an initial step that just applies key addition and shortened last round without bit permutation.

$E(x : \{0,1\}^{mn}, k : \{0,1\}^s) : \{0,1\}^{mn}$
1. *initial white step (round key addition)*
   $u = x \oplus K(k, 0)$
2. $r-1$ *regular rounds*
   for $i = 1$ to $r-1$ do
   a. *word substitutions*
      for $j = 0$ to $m-1$ do
         $v^{(j)} = S(u^{(j)})$
   b. *bit permutation*
      $w = v^\beta$
   c. *round key addition*
      $u = w \oplus K(k, i)$
3. *shortened last round (without bit permutation)*
   for $j = 0$ to $m-1$ do
      $v^{(j)} = S(u^{(j)})$
   $y = v \oplus K(k, r)$; return $y$



**Known Attacks**:

- Brute Force Attack
- Linear Cryptanalysis
- Differential Cryptanalysis

**Linear Cryptanalysis**:

- Relies on a set $T$ of plaintext-ciphertext pairs
- Instead of brute forcing the whole key, get small parts of the key at a time
- TODO

**AES (Advanced encryption standard)**: basically SPCS with modifications