TeComp
Strengthening Teaching Competences
in Higher Education
in Natural and Mathematical Sciences
FAN S. NOLI
Co-funded by the
Erasmus+ Programme
of the European Union

Modern Cryptography: Teaching Challenges

Blerina Çeliku
Department of Informatics

Cryptography Goals

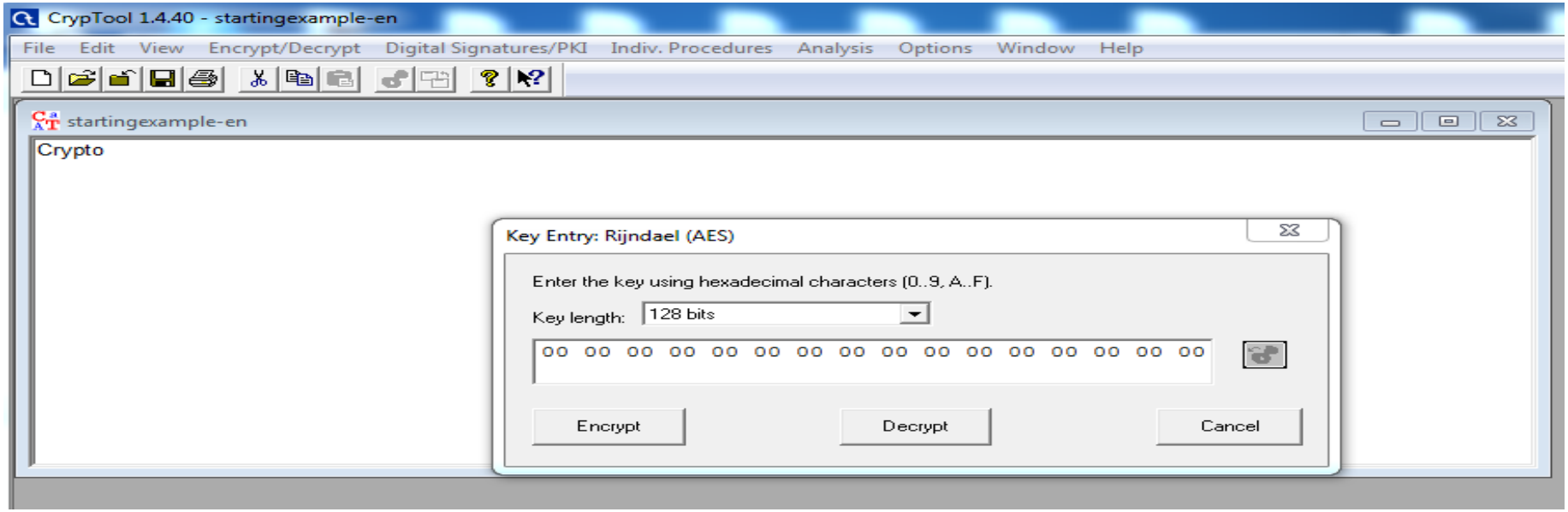
- Confidentiality
- Identification & Authentication (SHA-3, ECDSA)
- Integrity
- Non-Repudiation

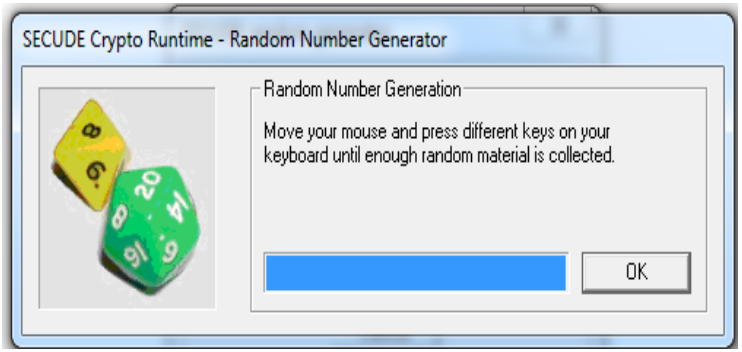
Fundamentals of Crypto

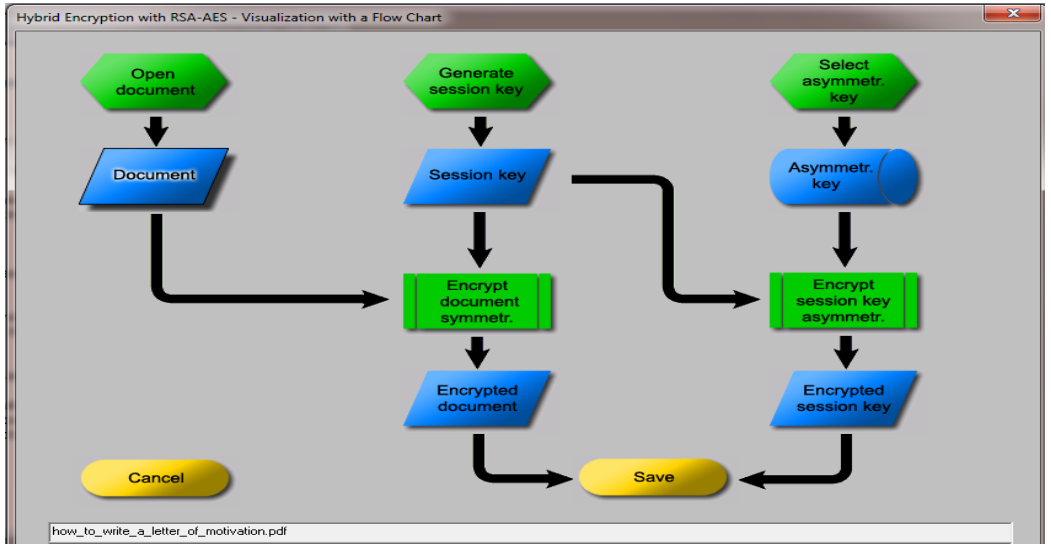
- Symmetric Key Algorithms
- Asymmetric Key Algorithms
- Hash Functions (digest values)
- Digital Signatures
- Encryption
- Decryption
- Attacks

Tools & Tasks

- ✓ Camtasia Studio
- ✓ Interactive Videos
- ✓ Posters
- ✓ Animations
- ✓ Knowledge Clips
- ✓ CrypTool Portal, https://www.cryptool.org/en/ct1
- ✓ FolderLock
- ✓ …

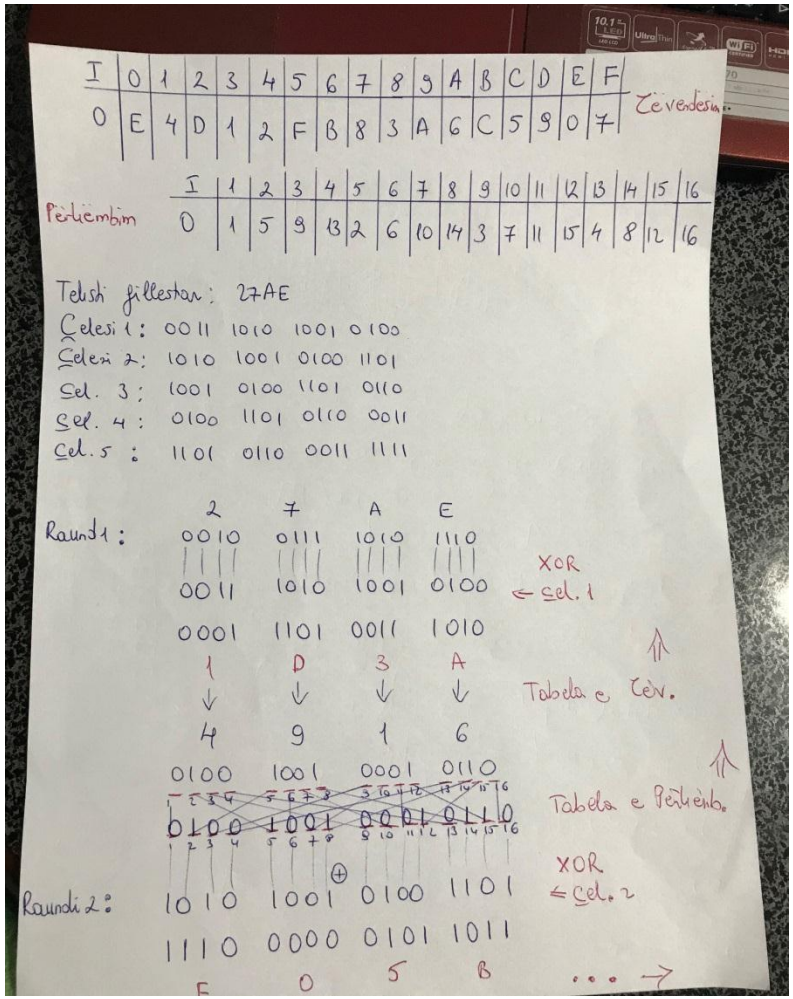

CrypTool 1.4.40 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Crypto
Key Entry: Rijndael (AES)
Enter the key using hexadecimal characters (0..9, A..F).
Key length: 128 bits
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Encrypt
Decrypt
Cancel

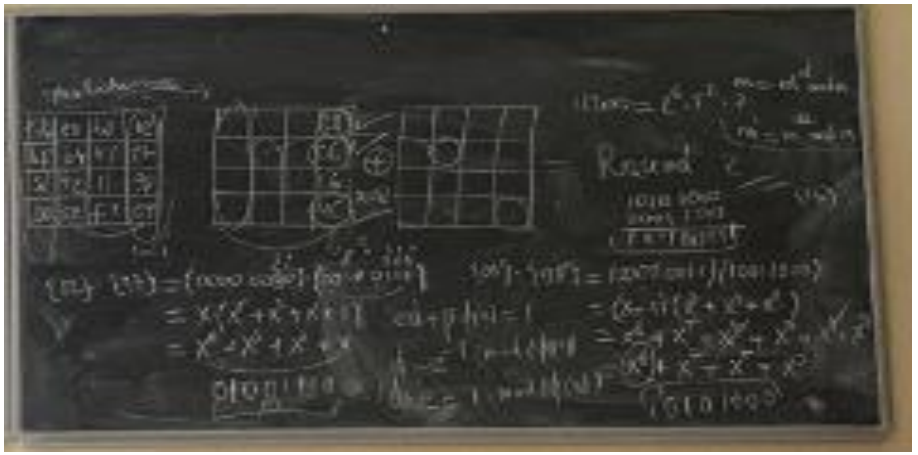

SECUDE Crypto Runtime - Random Number Generator
Random Number Generation
Move your mouse and press different keys on your keyboard until enough random material is collected.
OK


Hybrid Encryption with RSA-AES - Visualization with a Flow Chart
Open document
Document
Generate session key
Session key
Select asymmetr. key
Asymmetr. key
Encrypt document symmetr.
Encrypt session key asymmetr.
Encrypted document
Encrypted session key
Cancel
Save
how_to_write_a_letter_of_motivation.pdf

SP Networks

1.



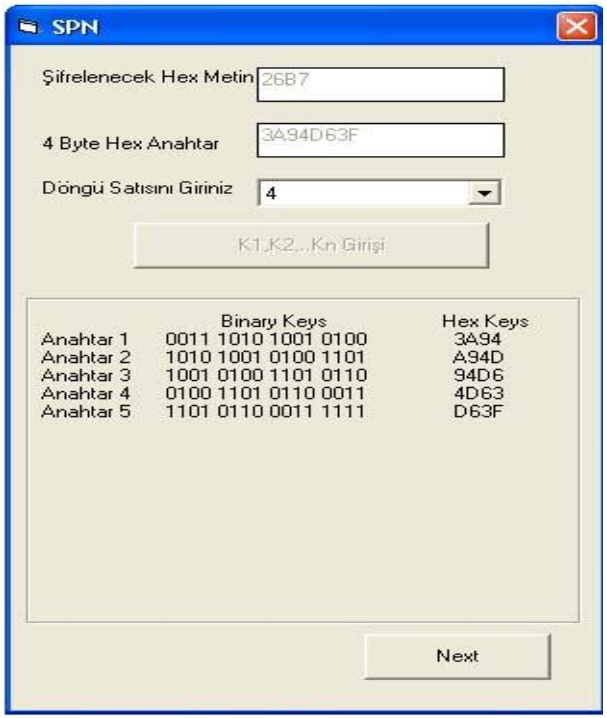


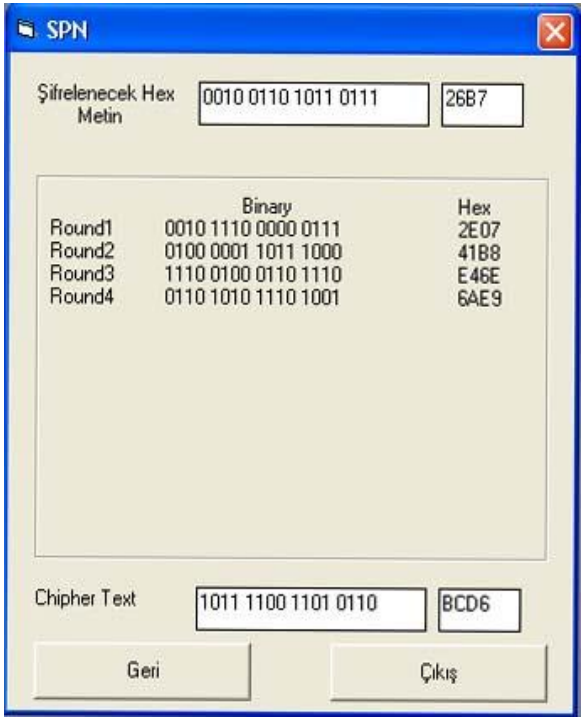
2.

SPN Code Works

Sbox

a,b	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	10	6
A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	6	8
F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8





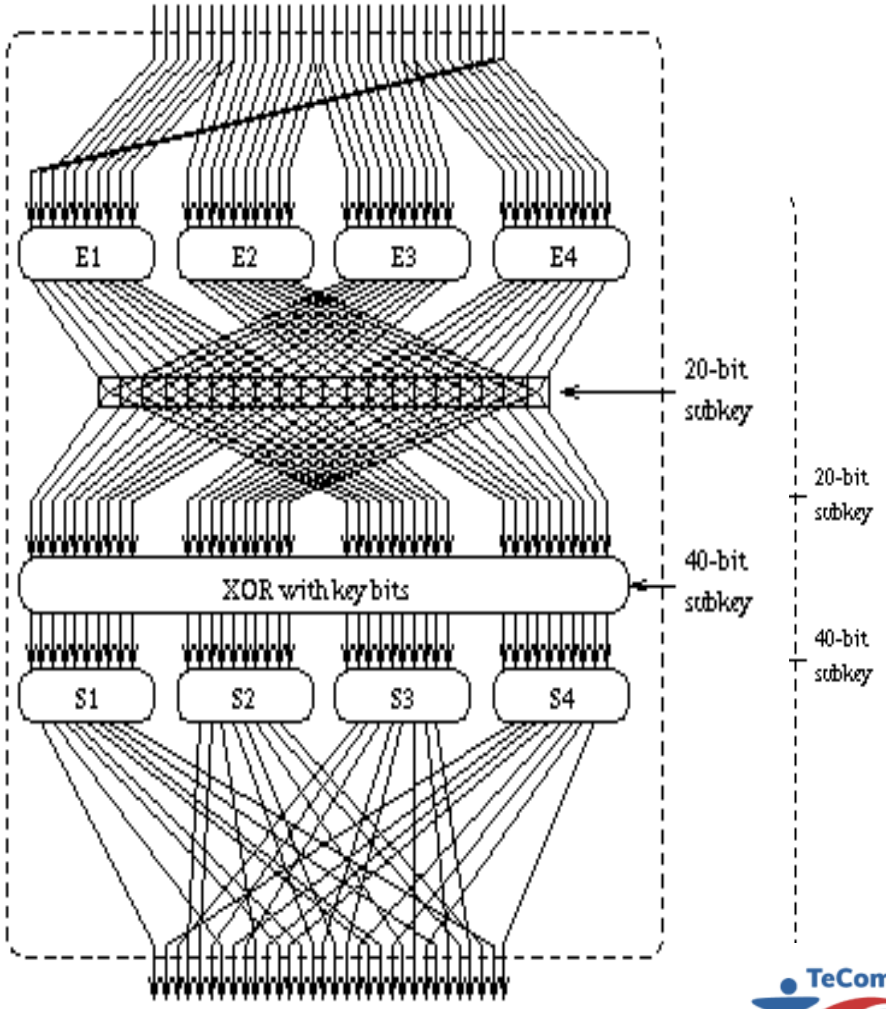
SPN (16 bit) Animations

3.

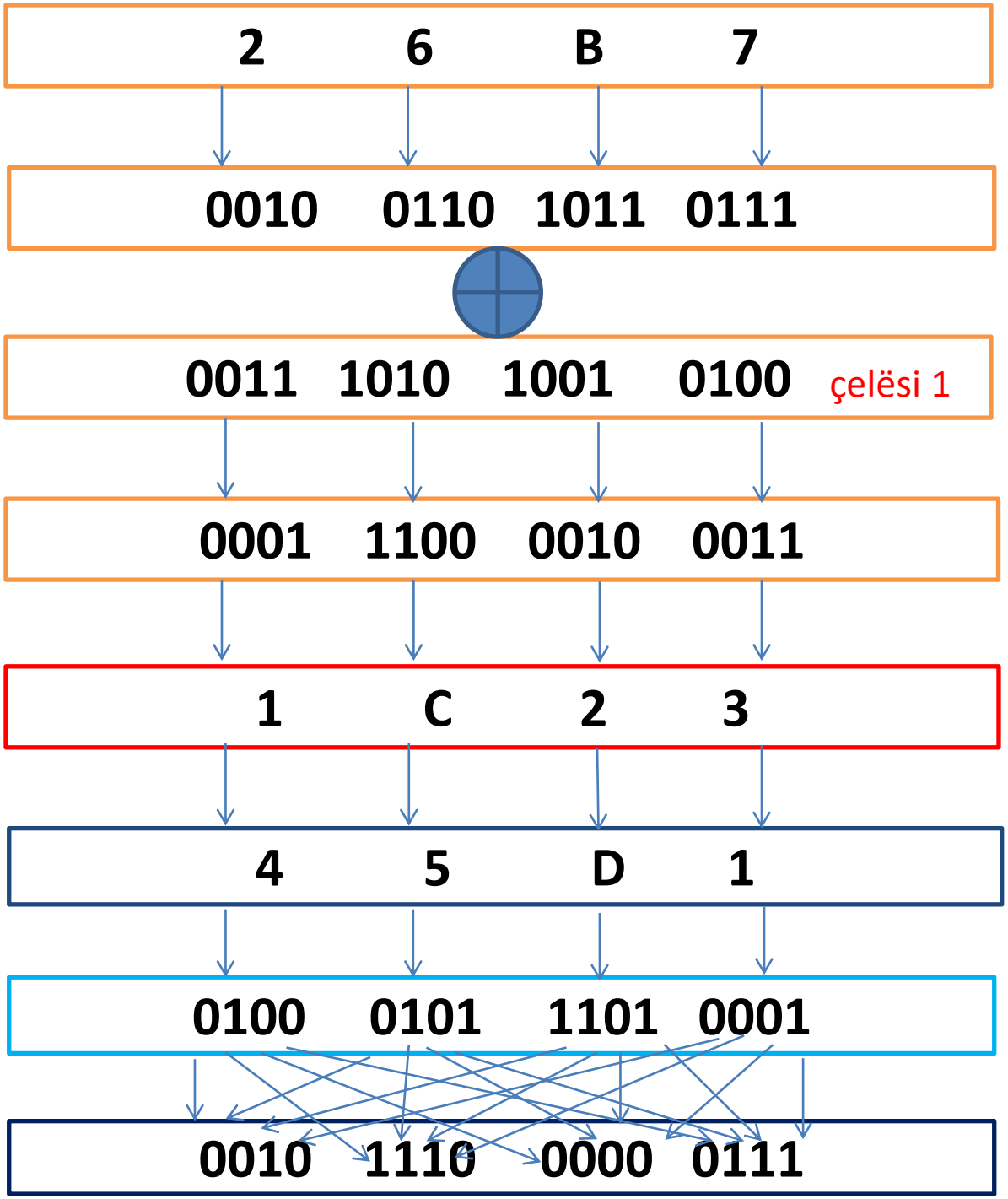
The “bone structure” of many algorithms, such as AES etc.

The basic operations:

- ✓XOR-Mixing Keys
- ✓Substitution
- ✓Permutation



SP



I	O
0	E
1	4
2	D
3	1
4	2
5	F
6	B
7	8
8	3
9	A
A	6
B	C
C	5
D	9
E	0
F	7

Zëvendësim

Përkëmbim

I	O
1	1
2	5
3	9
4	13
5	2
6	6
7	10
8	14
9	3
10	7
11	11
12	15
13	4
14	8
15	12
16	16

Thank you!

https://teams.microsoft.com/_#/school/files/Cryptography_Lectures/