IK2206 – Internet Security and Privacy
Assignment 1

Exercise 1
Alice has designed an 8-bit pseudo-random number generator using the following linear congruential generator algorithm:
$R_{i+1} = (69 \times R_i + 113) \bmod 256$

She uses the output from the algorithm to encrypt a message by a bitwise XOR operation of the message and the output of the generator.

Suppose that Alice wants transmit the ASCII string “Safe” as plaintext message to Bob, and uses $R_0 = 43$ as the initial value for the generator. What is the resulting ciphertext? (She encrypts the string character by character, going from left to right.)

The ciphertext is, most likely, not going to be readable in ASCII, so you should use hexadecimal notation for your answer. Give your answer as a sequence of bytes in hexadecimal notation, with a space between bytes. For example, "07 A6 FB 93".

Calculating the key
(69 × *43* + 113) mod 256 = 8
(69 × *8* + 113) mod 256 = 153
(69 × *153* + 113) mod 256 = 174
(69 × *174* + 113) mod 256 = 87

Encryption

ASCII Char	**S**	**a**	**f**	**e**
Plaintext (Hex)	53	61	66	65
Plaintext (Bin)	01010011	01100001	01100110	01100101
Key (Dez)	8	153	174	87
Key (Bin)	00001000	10011001	10101110	01010111
XOR Encryption (Bin)	01011011	11111000	11001000	00110010
XOR Encryption (Hex)	5B	F8	C8	32

http://www.krisl.net/cgi-bin/ascbin.pl

Exercise 2
How would you characterize the encryption system that Alice has designed?
Choose one answer.

- ○ A. Block cipher with public key
- ○ B. Block cipher with symmetric key
- ○ C. Stream cipher with public key
- ◉ D. Stream cipher with symmetric key

Exercise 3
What key is used in Alice's encryption scheme above? (Give a numerical value for your answer.)
43.0

Exercise 4

When a block cipher is used to encrypt a large message, it can be run in a "mode of operation". Which of the following are true:

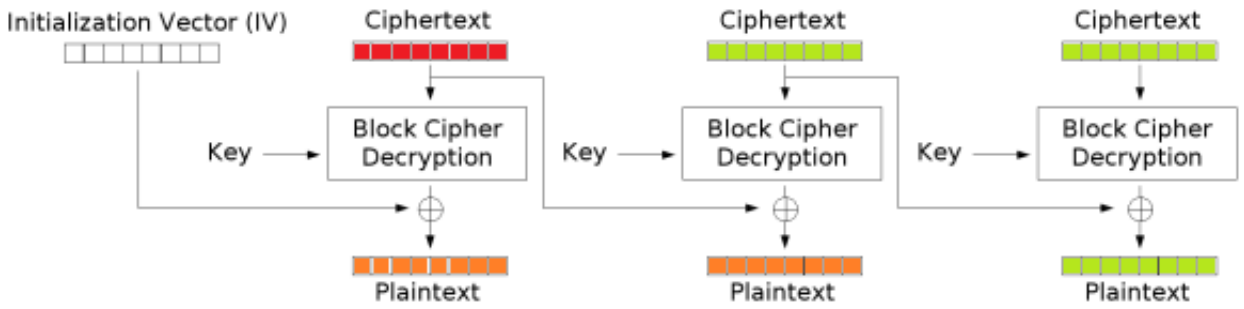
- [x] A. An initialisation vector can be used to create randomness so that identical messages will generate different ciphertexts
- [ ] B. With ECB mode, the mapping of a block depends on the previous blocks
- [x] C. CBC mode protects against attacks where the attacker reorders the blocks in the ciphertext
- [ ] D. With CBC mode, identical plaintext blocks are mapped to identical cipherblocks
- [ ] E. With CBC, if a ciphertext block is modified, the corresponding plaintext block will be affected after, as well as all plaintext blocks that follow [1]
- [ ] F. An initialisation vector can be used to increase the key length
- [ ] G. If CBC is used without an initialization vector, or with an initialization vector set to zero, the security is no better than that of EBC
- [x] H. ECB mode performs the same block cipher operation on each block

Exercise 5

Which of the following statements about DES (Data Encryption Standard) are true?

- [ ] A. DES is a public key algorithm
- [ ] B. The key size of 3DES is three times the key size of standard DES [2]
- [x] C. 3DES consists of running DES multiple times
- [x] D. The decryption operation basically consists of running encryption backwards
- [ ] E. The transformation of a block is variable, depending on the position of the block in the sequence
- [x] F. The short key length in standard DES makes it vulnerable to brute-force attacks
- [x] G. In practice, DES should be used in a mode of operation in order to be secure

[1] In case of a corrupted CBC-ciphertext, only two plaintext blocks are affected: the corresponding block and the block after. All further blocks are not affected.



[2] DES uses an encryption key of 56bits length. 3DES keys are twice as long, 112bits. But it is possible to run 3DES in a 3-key mode, where a total key length of 168bits is used.

Exercise 6

A PKI certificate is:

- ○ A. A name and a private key signed using the public key of a certificate authority
- ○ B. A name and a private key signed using the private key of a certificate authority
- ◉ C. A name and a public key signed using the private key of a certificate authority
- ○ D. A name and a public key signed using the public key of a certificate authority

http://en.wikipedia.org/wiki/Public_key_infrastructure

Exercise 7

Which of the following statements about certificate revocation are true?

- ☐ a. Certificates are only revoked because they are compromised. [3]
- ☐ b. Delta-CRLs make CRL distribution more secure.
- ☑ c. Certificate expiration help making CRLs more manageable.
- ☑ d. Online revocation servers are preferable to offline CRLs.
- ☑ e. CRLs listing valid certificates are more secure than CRLs listing revoked certificates.

Exercise 8

Which of the following statements about public key algorithms are true?

- ☐ a. The RSA algorithm is suitable for encryption/decryption of bulk data.
- ☐ b. Diffie-Hellman key-exchanges can replace an RSA-based PKI.
- ☑ c. The RSA algorithm relies on an unproven assumption for its security. [4]
- ☐ d. Using RSA public keys protects you against man-in-the-middle attacks.
- ☐ e. Diffie-Hellman can be used for authentication.

http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[3] Also if the owner information change or if the issuer has become untrustworthy for any reason.

[4] The real premise behind RSA's security is the assumption that factoring a big number is hard. The best known factoring methods are really slow. To factor a 512-bit number with the best known techniques would take about thirty thousand MIPS-years.
(Source: Network Security: Private Communication in a Public World (2nd Edition), by C. Kaufman, R. Perlman, M. Speciner)

Exercise 9

Alice wants to use RSA to encrypt the message *M*=88 and send it to Bob. Bob has chosen two prime numbers (*p*=17 and *q*=11) to calculate the public number needed for the RSA keys. Furthermore, Bob has selected the number *e*=7 to use in his public key.

What is the resulting public key published by Bob? Give the answer in the format {n, e}, where n and e are numerical values.

e = 7
n = p*q = 17*11 = 187
The answer to this question is: {187, 7}

Encryption: Alice encrypts message m with Bob's public key {n, e}:
$c = m^e \bmod n = 88^7 \bmod 187 = 11$

Decryption: Bob decrypts with his private key {n, d}:
$\phi(n) = (p - 1)(q - 1) = (17 - 1)(11 - 1) = 160$
$d = e \bmod \phi(n) = 7 \bmod 160 = 7$
$m = c^d \bmod n = 11^7 \bmod 187 = 88$

http://en.wikipedia.org/wiki/RSA_(algorithm)
https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html

Exercise 10

Alice wants to communicate with Bob in a secure way, using symmetric key cryptography. She encrypts the message with a secret key shared by Alice and Bob. She sends the ciphertext message together with the plaintext message to Bob. Assuming that no one except for Alice and Bob has access to the secret key, what kind of security would Alice and Bob achieve in this way?

- ☐ A. None
- ☐ B. Confidentiality
- ☑ C. Integrity [5]
- ☑ D. Authenticity

Exercise 11

Which of the following are properties of a well-designed secure hash function for message authentication?

- ☑ A. It should be difficult to find two different messages with the same hash
- ☐ B. A small change in the message should give a small change in the hash
- ☑ C. Given a hash value, it is difficult to compute the corresponding message [6]
- ☐ D. Two different messages cannot have the same hash
- ☐ E. If the same message is used as input more than once, it should generate different hash values
- ☐ F. A small change in the message gives a small change in the hash

[5] If the plaintext or the ciphertext message is tampered with, or both, the messages will not match when Bob decrypts the ciphertext and compares it to the plaintext.

[6] Hash functions are so called „irreversible functions". Another term is "one-way function".

Exercise 12

What could it mean when cryptologists say that a hash algorithm has “security weaknesses”?

- [ ] A. The details of the hash algorithm have been revealed to the public
- [x] B. There are mathematical methods to find two messages with the same hash, and those methods are faster than brute-force
- [x] C. There are mathematical methods to compute the message from the hash value, and those are faster than brute-force
- [ ] D. There are mathematical methods to compute the hash value from the message, and those methods are faster than brute-force
- [ ] E. The hash algorithm can be efficiently computed in a short time, which makes it possible to stage a brute-force attack