20872 43

Test Pearl 100 — Cryptography

Pearls of Computer Science (201300070)
5 October 2018, 13:45–14:45
Module coordinator: Doina Bucur
Instructor: Andreas Peter

- You may use 1 A4 sheet with your own notes for this test, as well as a *simple* calculator
- Scientific or graphical calculators, laptops, mobile phones, books etc. are not allowed. ***Put those in your bag now (with the sound switched off)!***
- Always motivate/explain your answers, unless it is explicitly stated not to!
- Total number of points: 38

14 points **Question 1** Write down your answers (A, B, C, or D) on your answer sheet and **NOT** on the exam sheet at hand. There is only **one correct answer per subquestion**. Your answers require no motivation.

IMPORTANT: Don't just guess; for each wrong answer, you get 1 point deducted!

(a) Let `JVVIMQ` be a ciphertext produced by the Vigenère cipher using the key `PIN`. Which of the following is the underlying plaintext?
   A. `ATTACK`
   B. `DEFEND`
   C. `UNITED`
   D. `CRYPTO`

(b) According to the second Kerckhoffs' principle, which of the following statements is correct?
   A. The secret key used in a secret-key encryption scheme must be able to fall into the hands of the enemy without inconvenience.
   B. The public key used in a public-key encryption scheme must be able to fall into the hands of the enemy without inconvenience.
   C. The source code of the implementation of an encryption scheme must **not** be able to fall into the hands of the enemy.
   D. The output of an encryption scheme (i.e., a ciphertext) must **not** be able to fall into the hands of the enemy.

(c) Suppose that Alice encrypts the plaintext `000` using the One-Time-Pad. Assuming that you don't know which key Alice used in the encryption, what is the probability that `000` is the resulting ciphertext?
   A. 0%
   B. 6.25%
   C. 12.5%
   D. 25%

(d) What is the concept of "hybrid encryption"?
   A. First use a secret-key encryption scheme to exchange a key, then use this key in a public-key encryption scheme.
   B. First encrypt a given message with a secret-key encryption scheme, then produce a public-key signature on the resulting ciphertext.
   C. First use a public-key encryption scheme to exchange a key, then use this key in a secret-key encryption scheme.
   D. First produce a public-key signature on a given message, then encrypt the resulting signature with a secret-key encryption scheme.

(e) Let $p = 31$ and $q = 43$ be primes, and $N = pq = 1333$. What is the result of the computation: $(1234^{1260} + 2567) \bmod 1333$?
   A. 1232
   B. 1233
   C. 1234
   D. 1235

(f) Which elements are contained in $\mathbb{Z}_{12}^*$?
A. $1,5,7,11$
B. $0,1,5,7$
C. $3,5,7,11$
D. $1,3,5,7$

(g) Which of the following numbers is a valid (= generated as described in the lecture), but too small to be secure, RSA modulus?
A. $N=9$
B. $N=29$
C. $N=1024$
D. $N=1271$

7 points **Question 2** Consider the following keyed-function

$$F:\{0,1\}^2\times\{0,1\}^2\to\{0,1\}^2 \quad \text{whereas} \quad F(K,x)=K\oplus x.$$

Decrypt the 4-bit ciphertext $c=1101$ using the Feistel cipher with 3 rounds, above keyed-function F, and the round-keys $K_0=11$, $K_1=10$, and $K_2=01$.

9 points **Question 3** Consider the following plaintext message (a 5-bit string)

`11010`

Encrypt this message in the CBC-mode by using the following 2-bit block cipher

$$\mathsf{E}_k(b_1b_0)=b_1b_0\oplus k$$

with the bit-string $k=\texttt{10}$ as secret key (note that b_1b_0 denotes an arbitrary 2-bit plaintext message). As initialization vector for the CBC-mode, use the bit-string $IV=\texttt{11}$.

8 points **Question 4** Let $p=37$, $q=41$, and $N=pq=1517$. Assume that we use $(N,e)=(1517,823)$ as the public key in the RSA signature scheme.

(a) Compute Euler's totient function $\varphi(N)$.

(b) Compute the RSA secret key $d\geq 0$ that corresponds to the public key $(N,e)=(1517,823)$. The following table with some pre-computed calculations might be helpful (as it avoids the need to compute the extended Euclidean algorithm):

A.	$\gcd(p,q)=1$	E.	$1=1440\cdot197+1517\cdot(-187)$
B.	$\gcd(\varphi(N),N)=1$	F.	$1=37\cdot10+41\cdot(-9)$
C.	$\gcd(\varphi(N),e)=1$	G.	$1=1517\cdot(-319)+823\cdot588$
D.	$\gcd(N,e)=1$	H.	$1=1440\cdot(-4)+823\cdot7$

(c) Sign the message $m=2$ using the RSA signature scheme with the in (b) computed secret key $d\geq 0$ (if you couldn't solve (b), then use the key $d=11$, which is different from the correct result in (b)!).