1. (a) Sistemul OTP sigur permite folosirea unei singure chei de criptare pentru ~~mai multe mesaje diferite~~ **UN SINGUR MESAJ** atata timp cat lungimea cheii este cel putin la fel de mare ca lungimea mesajelor. (2p) **F**
2. (b) Este recomandat sa se foloseasca AES pentru transmiterea fisierelor de dimensiuni mari. (2p) **A**
3. (c) Pentru schimbul de chei Diffie-Hellman ~~este esential ca cele doua parti sa partajeze ın avans un secret.~~ **F** -Se creaza o cheie secreta fara ca cele doua parti sa partajeze ın avans un secret.
4. (2p) (d) Pentru a asigura ~~integritatea~~ confidentalitatea mesajelor, este suficient sa le trimitem criptate cu un sistem de criptare public si sigur. (2p) **F**
5. (e) La crearea semnaturilor digitale, are mai mult sens mai ıntai sa semnam mesajul si apoi sa ıl comprimam cu o functie hash **F.** hash first, sign after
6. (f) Timpul necesar unui atacator pentru a gasi coliziuni pentru functia hash SHA-256 este de ~~2^256~~ **F 2^128**
7. (g) Nerepudierea ıi permite lui Bob sa prezinte spre verificare unei terte parti un document semnat de Alice si această proprietate este asigurata numai de ~~codurile de autentificare a mesajelor (MAC).~~ (2p) schema de semnatura digitala
8. (h) Combinația ~~autentifica-apoi-cripteaza~~ este ıntotdeauna sigura indiferent de cum sunt instantiate componentele ei. (2p) cripteaza-apoi-autentifica
9. (i) Sistemele de criptare post-cuantice sunt sisteme de criptare care folosesc metode ~~cuantice~~ pentru asigurarea securitatii ın fața unui adversar ~~clasic~~. (2p) clasice, cuantic
10. (j) Protocolul TLS este folosit de catre browser-ul web de fiecare data cand realizeaza o conexiune sigura cu un site web folosind ~~http~~. (2p) https

EX 2

a. Daca se stie ca o parola are exact 6 caractere, aceasta este reprezentata pe 48 de biti si hash 48+8=56. Aceasta poate fi usor aflata de un atacator pasiv printr-un atac de tip brute-force. PRNG-ul nu este safe deoarece informatia primita ca seed nu estte pseudo aleatoare, ceea ce ofera un avantaj adversarului.
b. RSA- usor atacabil iar N ul fiind 128 adica mic este usor facorizabil in factori primi. Singurul rsa cunoscut ca fiind safe este n 2048.
c. O alta vulnerabilitate gasita la nivel de integritate este lipsa de tls, mac sau semnături digitale la criptarea mesajelor interne tramise pe chat. Fara acestea, nu se poate asigura integritatea mesajelor. Alta prob de securitate faptul ca problema log discret folosit in protocolul de schimb de chei D-H este usoara, aceasta fiind vulnerabil. Daca informatia este aflata atunci securizarea comunitatea interne nu mai exista.

EX 3

a. Functia Fki trebuie sa fie o functie pseudoaleatoare(PRF). Functia trebuie sa fie o functie bijectiva(inversabila)
b.

ci = Fk2 (ci−1 ⊕ Fk1 (mi−1 ⊕ mi)) | Fk2^-1
Fk2^-1(ci) = ci-1 ⊕ Fk1 (mi−1 ⊕ mi)
ci-1 ⊕Fk2^-1(ci)= Fk1 (mi−1 ⊕ mi) | Fk1^-1
Fk1^-1(ci-1 ⊕Fk2^-1(ci)) = mi-1 ⊕ mi
mi= mi-1 ⊕ Fk1^-1(ci-1 ⊕Fk2^-1(ci))

c. 2^16 (m0,c0)
d. N-i+1 blocuri

EX 4
Mac′ (k,(m1, m2)) = Mac(k, m1 ⊕ m2)
Vrfy′ (k,(m1, m2), t) = Vrfy(k,(m1, m2), t)

Fie m3 si m4 ai m3 ⊕ m4 = m1 ⊕ m2. =>Mac′ (k,(m3, m4)) = Mac′ (k,(m1, m2)) si Vrfy′ (k,(m3, m4), t) = Vrfy(k,(m1, m2), t) => Adversarul obtine un tag valid pentru un mesaj netrimis la oracol => Mac nu e sigur