Praktikum 4

https://courses.cs.ut.ee/2024/turve/spring/Main/Praktikum4

ÜL 1


```
Delivered-To: rivik.richard@gmail.com
Received: by 2002:a05:7000:79c8:b0:55c:e7c2:f41c with SMTP id p8csp520471maz;
        Mon, 11 Mar 2024 08:11:48 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IFAuVJujUb6nF3YL6ForsRB9DNgIWv5IQyH61yxDXfjrWJ6dBg4picpsFwBLbfP6ILf+UdL
X-Received: by 2002:a50:a6d4:0:b0:565:dfac:a686 with SMTP id f20-20020a50a6d4000000b00565dfaca686mr4158477edc.38.1710169908352;
        Mon, 11 Mar 2024 08:11:48 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1710169908; cv=none;
        d=google.com; s=arc-20160816;
        b=hg0dubIl0OmseOv22HwWH/zSgCf/AqSKbeYptMvSK3dflY4FnqrCx+C65WjQqmfQSZ
         EWyJfhKzvVogq2dprAW3d87VQSdBUQ475VX6GOPAzrf7A/PU4waPEguMd9BqA9No9a/0
         g06PdpoZF6oqznC6HpktnsWPKLMjH0YsYYQojK4xpd98XBqtNmB6I9BA2SW2GC9clwb+
         3onMXu64OTHmGLtB0FeBkOFYN13XBzZnjyyZa0RVUEnuxlXQhfbvRkajwNABsEggEFnl
         yO4vl9FHYXzahaBWJnUhgQNMdvOhZTUC9e4eKlfBmhx0VtvSvEfHBxYVvNHYEWLHf910
         nSRw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=subject:to:from:dkim-signature:dkim-filter:message-id:date;
        bh=HbQ0Ip/zSbkVtazaOi9u7L1BCfCloyfs4POn4Khdikc=;
        fh=ifd+X9MYiu4J04ZvnNET3iDTjD0r2Q5Bpyn/1CgPbDs=;
        b=Syqz6OxxFJDyrTqPSC4mGatVJEDQxux9h+a6OxLW7uhk1nhgCXAcgN5KvSRMaR2fzc
         tIr+AwIR4xHeuaMO6PrsQNNdO+jA5UpOUeG0YeBXDl7gCIw14PQgOYodBGbFH+q1R0mg
         kwXZLVbcfwA3puI7Yn0u7itFaq4w8RRwjjEYKcmn2yIbSUyhOlcNug/bMoHLiuSRflbj
         iPUWKvpaDmQfhfyRqpTTKYW7hTXqldsvklvAft+++3EGSdxNodaJyBb+DzBWIAjToNxG
         vC+Ct8nXR8cYfCnkcfRwEIKVt+NM4SP26oB2/7nxEj7TNTAkJ+EvgLDZjNw5EfUCeNP
         nORA==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@ut.ee header.s=selektor1 header.b=BcyC6hI5;
       spf=pass (google.com: domain of alo.peets@ut.ee designates 2001:bb8:2002:500::46 as permitted sender) smtp.mailfrom=alo.peets@ut.ee;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=ut.ee
Return-Path: <alo.peets@ut.ee>
Received: from smtp1.it.da.ut.ee (smtp1.it.da.ut.ee. [2001:bb8:2002:500::46])
        by mx.google.com with ESMTPS id dz12-20020a0564021d4c00b005675328a3basi25588S5edb.300.2024.03.11.08.11.48
        for <rivik.richard@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Mon, 11 Mar 2024 08:11:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of alo.peets@ut.ee designates 2001:bb8:2002:500::46 as permitted sender) client-ip=2001:bb8:2002:500::46;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@ut.ee header.s=selektor1 header.b=BcyC6hI5;
       spf=pass (google.com: domain of alo.peets@ut.ee designates 2001:bb8:2002:500::46 as permitted sender) smtp.mailfrom=alo.peets@ut.ee;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=ut.ee
Date: Mon, 11 Mar 2024 08:11:48 -0700 (PDT)
Message-ID: <65ef1f34.050a0220.9e9dc.87d2SMTPIN_ADDED_MISSING@mx.google.com>
DKIM-Filter: OpenDKIM Filter v2.11.0 smtp1.it.da.ut.ee 927D2602D0
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=ut.ee; s=selektor1; t=1710169907; bh=HbQ0Ip/zSbkVtazaOi9u7L1BCfCloyfs4POn4Khdikc=; h=From:To:Subject:From; b=BcyC6hI5kjglkxDZTxVacAkohfME6oMfXLcUSUD3+XM8qAV+oK1EkEaZj19aTPkIg
         geyi10SJJ1mDa5EkX2Dtk/HCihKc3Gaoc2EtLxLQ3S+XMtkE6XVQEYxZaQpt9HC4Ge
         sI4cBl6aQBBO117HyJtkEIUJNeCfpO3kOJ3HCM5Q7CqhVlVcywMVPwI6C+HsomFPqz
         3FW+VpiGXa13hibe7XJvdpQSZ+Iab1T14x/drQDpnM0rwwrhFo3TBZcfmyY93dRup
         JoFy2duCkhIMo469DPMmJ3BSTioYQwlPtDTOXvdet4337oB2yp6glnLKNx4L6P4fZ3
         clPSqmXtzLPIg==
Received: from ut.ee (adalberg.ut.ee [IPv6:2001:bb8:2002:500::36]) by smtp1.it.da.ut.ee (Postfix) with SMTP id 927D2602D0 for <rivik.richard@gmail.com>; Mon, 11 Mar 2024 17:08:14 +0200 (EET)
From: Alo Peets <alo.peets@ut.ee>
To: Richard-Sven Rivik <rivik.richard@gmail.com>
X-Mailer: telnet
Subject: e-maili test Turve2024
Content-Type: text/plain; charset=UTF-8

Käesolev kiri on saadetud telneti vahendusel ja illustreerib kuidas saata võõra nime ja aadressi alt e-maili.
```


ÜL 2

```
kasutaja@rivik: ~
File  Edit  View  Search  Terminal  Help
kasutaja@rivik:~$ ssmtp -v richard-sven.rivik@ut.ee < mail.txt
[<-] 220 AS4P189CA0034.outlook.office365.com Microsoft ESMTP MAIL Service ready at Mon, 11 Mar 2024 15:30:21 +0000
[->] EHLO rivik
[<-] 250 SMTPUTF8
[->] STARTTLS
[<-] 220 2.0.0 SMTP server ready
[->] EHLO rivik
[<-] 250 SMTPUTF8
[->] AUTH LOGIN
[<-] 334 VXNlcm5hbWU6
[->] YW5kbWV0dXJ2ZS5saWJha29udG9Ab3V0bG9vay5jb20=
[<-] 334 UGFzc3dvcmQ6
[<-] 235 2.7.0 Authentication successful
[->] MAIL FROM:<alo.peets@ut.ee>
[<-] 250 2.1.0 Sender OK
[->] RCPT TO:<richard-sven.rivik@ut.ee>
[<-] 250 2.1.5 Recipient OK
[->] DATA
[<-] 354 Start mail input; end with <CRLF>.<CRLF>
[->] Received: by rivik (sSMTP sendmail emulation); Mon, 11 Mar 2024 17:30:21 +0200
[->] Date: Mon, 11 Mar 2024 17:30:21 +0200
[->] To: Richard-Sven Rivik  <richard-sven.rivik@ut.ee>
[->] Subject: Andmeturve e-mail SSMTP vahendusel
[->] From: Alo Peets <alo.peets@ut.ee>
[->] Content-Type: text/html; charset="utf8"
[->]
[->] <html>
[->] <body>
[->]
[->] Käesolev kiri on saadetud asurealt SSMTP abiga ja kasutasime selles Microsofti e-maili servereid. Tegevus illustreerib kirja saatmise parameetrite modifitseerimist käsurealt.
[->]
[->] <br>Andme Turve
[->] <br>kursus 2024
[->] </body>
[->] </html>
[->] .
[<-] 554 5.2.252 SendAsDenied; andmeturve.libakonto@outlook.com not allowed to send as alo.peets@ut.ee; STOREDRV.Submission.Exception:SendAsDeniedException.MapiExceptionSendAsDenied; Failed to process message due to a permanent exception with message [BeginDiagnosticData]Cannot submit message. 0.35250:4D230000, 1.36674:0A000000, 1.61250:00000000, 1.45378:02000000, 1.44866:60360000, 1.36674:0E000000, 1.61250:00000000, 1.45378:65360000, 1.44866:36010000, 16.55847:FB130000, 17.43559:0000000024020000000000000000000000000000, 20.52176:140FC29C1F00001000000000, 20.50032:140FC29C8F17F01F07000000, 0.53414:14004A67, 0.35180:73230000, 255.23226:09000000, 255.27962:0A000000, 255.27962:0E000000, 255.31418:0A004967, 0.35250:140FC29C, 1.36674:0A000000, 1.61250:00000000, 1.45378:02000000, 1.44866:54000000, 1.36674:32000000, 1.61250:00000000, 1.45378:59000000, 1.44866:01000000, 16.55847:CF000000, 17.43559:00000000B80300000000000000000000000000, 20.52176:140FC29C1F0070201400FE67, 20.50032:140FC29C8F17101096230000, 0.53414:0B004536, 0.35180:03004E67, 255.23226:9F230000, 255.27962:0A000000, 255.27962:32000000, 255.17082:DC040000, 0.27745:80030400, 4.21921:DC040000, 255.27962:FA000000, 255.1494:0A000910, 0.38698:0F010480, 1.41134:47000000, 0.37692:87000000, 0.37948:87000000, 5.33852:00000000534D545000000100, 7.36354:0100000000000109874A159B, 4.56248:DC040000, 7.40748:0100000000000010BD1D3B72A, 7.57132:0000000000000000255F7983, 4.39640:DC040000, 1.63016:32000000, 8.45434:00003001E72BD5F0000000000000000BD796A02, 1.46798:04000000, 5.10786:0000000031352E32302E373336322E3033313A444239505230394D4236373433 3A6161383338323661 2D366661332D343266612D613261622D323132346562353532633166 3A3833373838 3A2E4E455420362E302E32
```

ÜL 3

1)
Kui “From:” rida ei ühti “smtp.mailfrom=” parameetriga, siis on saatja informatsiooni muudetud ning võib arvata, et kiri on vale
2)
Kui “SPF”, “DKIM”, “DMARC” kirjete juures on “fail”, mitte “pass”, siis e-mail on autentimise kontrolli läbikukkunud ning võib arvata, et kiri on vale
3)
Järgida “Received” kirjeid ning kontrollida kas teekond on normaalne
4)
Kontrollida, kas meilis esinevad ip-aadressid on seotud pahatahtlikke allikatega.
5)
Kõige lihtsam on kontrollida, kas e-maili sisu on harilik. Näiteks õigekiri, kirjastiil ning imelikud lingid ja manused

ÜL 5.2

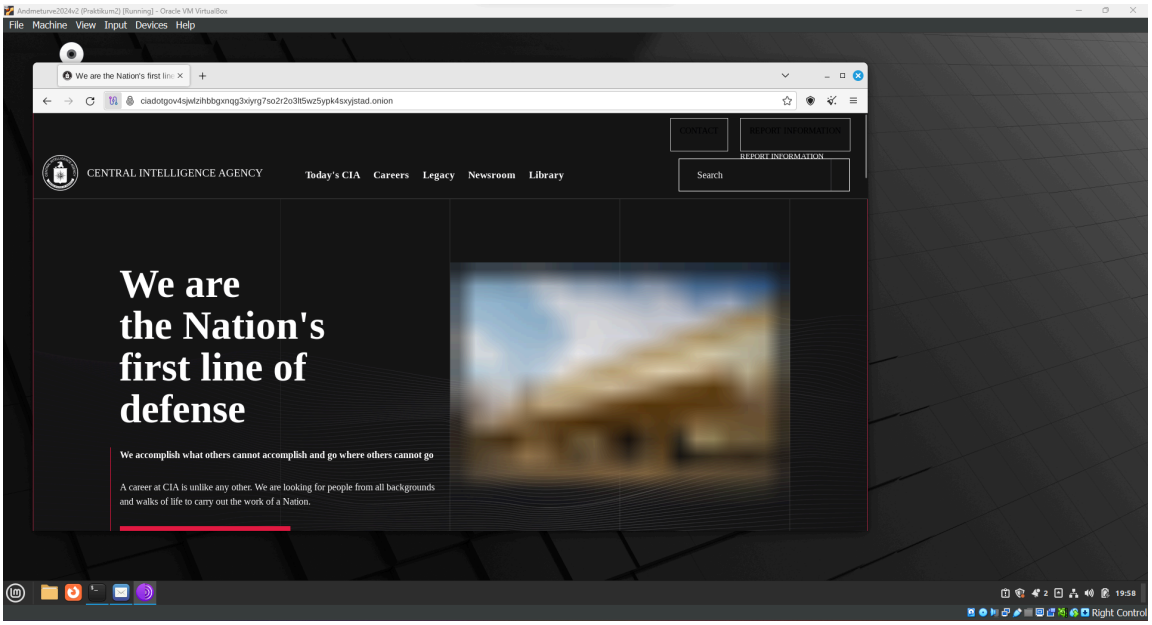
1)
Signalis on sõnumi otspunktkrüpteeritud ehk sisu on segatud ning seda saavad näha ainult saatja ja vastuvõtja. Tänu sellele on sisu privaatne ja turvaline.
SMS sõnumid ei ole otspunktkrüpteeritud. Näiteks võrgupakkuja, riigiorganid ja pahatahtlikud osapoolevad saavad SMS sõnumi edastust “pealt kuulata”.

2)
Signal krüpteerib ka metaandmeid, näiteks kes ja kuna saatis kellele. See tagab veel suurema privaatsuse.
SMS’ide puhul tavaliselt ei krüpteerita metaandmeid. Selle tõttu on paljud andmed, näiteks osapoolte telefoni numbrid, kellaajad, asukoha andmed kaitsmata. Metaandmete kaitse puudumine seab ohtu suhtluse privaatsuse ja anonüümsuse.

3)
Signalis on väga olulisel kohal ka autentimine ja kinnitamine. Kasutajad saavad turvanumbrite või QR-koodide abil kontrollida oma kontaktide identiteeti. See tagab, et nad suhtlevad õigete adressaatidega.

SMS sõnumitel aga puuduvad sisseehitatud mehhanismid saatja identiteedi kontrollimiseks või sõnumi terviklikkuse tagamiseks. See teeb SMS’id haavatavaks võltsimise ja andmepüügi rünnakute suhtes.

ÜL 6.1



Milliste andmete lekkimise eest riiklikele jälgimisasutustele TOR Browser veebilehitseja kasutamine aitab?

Asukohaandmed: kuna TOR varjab kasutaja originaalset IP-aadressi, siis aitab see kaitsta kasutaja asukohaandmeid. Jälgimisasutused ei saa võrguliikluse põhjal kindlaks teha kasutaja geograafilist asukohta.

Erinevate vestluste andmed: TOR pakub nt. meilide, sõnumite ja muude võrgusuhtluse tüüpidele otspunktkrüpteerimist. See takistab jälgimisasutustel sõnumite pealt kuulamist.