Web security and privacy - Final exam – 25 January 2019

FOR NON-ENGLISH: -2
USE A BALLPOINT PEN AND AVOID MICROSCOPIC CHARACTERS
UNREADABLE HANDWRITING: SKIPPED
You are kindly asked to deliver separate sheets for the two parts Web Security and Privacy

WEB SECURITY (prof. d'Amore) (time: 60 mins)

1. Email analysis

Examine the raw source that follows. **Select the header fields you consider relevant and discuss their values**, for the specific purpose of assessing the **trustworthiness** of the message.

```
X-Antivirus: avast (VPS 19011702)
X-Antivirus-Status: Clean
Delivered-To: damore@dis.uniroma1.it
Received: by 2002:a4a:a887:0:0:0:0:0 with SMTP id q7csp2167515oom;
        Thu, 17 Jan 2019 10:16:31 -0800 (PST)
X-Google-Smtp-Source: ALg8bN7SAt35xDC443gSYrzj9lXe9JKew6syisGLEDPn7TbBTVQrkmM55PEdgM+4SwB6A7fZXQcJ
X-Received: by 2002:a2e:9b52:: with SMTP id o18-v6mr10195715ljj.108.1547748991183;
        Thu, 17 Jan 2019 10:16:31 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1547748991; cv=none;
        d=google.com; s=arc-20160816;
        b=V31sZ6Z+N0TRjbcenEseTJXdZp0X7/OFm0cEEq3cj51TA8PLUqO+Vmj/j3P3pFLvBN
        VtPImypYEbKqyOmeUUo7y3sFgTIE0C54OfGrV89gdSkCYcZyf4Ud95Tif7jDeIU8fC7M
        LBEta1+SwvRDkiZ9zqIV0PpSH4nkFNWhayFdEfsdcNtHgiv+EQKyiTQZz2rdWUKcNHFm
        HdBq3fLO3ioPs73bpV89Ibn37B7q5ErnL4Tke+1gBeNdYk/+XdU14veLQi2Z/8P2Egvd
        sXSy97Ul65ijiM5o6ZfyKDzxUvll5wXMwQDUaTXwuhLOFk7T7xXINGz2opEnoHSFs8GL
        enAQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:subject:date:reply-to:to:from
        :mime-version:message-id;
        bh=p4PaOZqumxPgM1cKvB272I4epAszCkEmAE12cunlPbw=;
        b=jY0lRgWBBnD3A9VjnSNhJMPFe4BgMMztxGwbqMJ+zVpso/9tgDZFLdHcNwnyaTf8vz
        C4dxncktrilBfKIj5PaLsbWmUPUc0G5CuJovXC5Ww9tSANzIfh0HB5PN0Zw95OXwxx/A
        K8zkWpOAKfoUcsc870Scm7i+64pYrcn+SzjaSBtGrrTgJMXkIHPLZnTRzQKutbfycTdN
        FCNKFJANN3TqI0Tfy3VEy99ZdllmTCwELKKGdHHtxFJAg2dq6AvnNGhhfZgvSxBO60p+
        wzJ0hof6aJd6hy1vEeDxwPzyYUpbKHysq5KVFjn66YLCEG8FbFdcj2Jmp5puZU0Bw6ie
        A4hg==
ARC-Authentication-Results: i=1; mx.google.com;
        spf=pass (google.com: best guess record for domain of info@kratos.ua designates 176.103.115.251 as
permitted sender) smtp.mailfrom=info@kratos.ua
Return-Path: <info@kratos.ua>
Received: from post.kratos.ua (post.kratos.ua. [176.103.115.251])
        by mx.google.com with ESMTPS id r203si23297971fe.145.2019.01.17.10.16.30
        for <damore@dis.uniroma1.it>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Thu, 17 Jan 2019 10:16:31 -0800 (PST)
Received-SPF: pass (google.com: best guess record for domain of info@kratos.ua designates 176.103.115.251 as
permitted sender) client-ip=176.103.115.251;
Authentication-Results: mx.google.com;
        spf=pass (google.com: best guess record for domain of info@kratos.ua designates 176.103.115.251 as
permitted sender) smtp.mailfrom=info@kratos.ua
Received: from WIN-4K804V6ADVQ (159.181.206.195.baremetal.zare.com [195.206.181.159])
    by post.kratos.ua with ESMTP
    ; Thu, 17 Jan 2019 18:22:28 +0200
Message-ID: <22DBCC0F-9361-4BDB-8189-B9C162C9DB29@post.kratos.ua>
MIME-Version: 1.0
From: "Poste Italiane" <info@kratos.ua>
To: damore@dis.uniroma1.it
Reply-To: info@kratos.ua
Date: 17 Jan 2019 08:22:28 -0800
```

```
Subject: =?utf-8?B?Tm900ZZmaWNhINCgb3N0ZdCg0LB5?=
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64

R2VudGlsZSBkYW1vcmVAZGlzLnVuaXJvbWExLml0PGJyPgo8YnI+CkNpIHJpc3VsdGEgdW4g
ZXJyb3JlIG5laSBzdW9pIFNlcnZpemkgT25saW5lLjxicj4KPGJyPgo8YSBocmVmPSJodHRw
czovL3Rpbnl1cmwuY29tL3k5MmZrdnRuIj5WZXJpZmljYSBhZGVzc288L2E+PC9ib2R5Pjwv
aHRtbD4=
```


2. Top 10 security risks - OWASP

Choose **one** of the top 10 security risks (OWASP 2017) as you like and describe: **attack vectors, weakness, impact** and **prevention**.

3. Public suffixes

Describe the Mozilla's project "Public Suffix List", explaining what type of data are collected and for what purpose(s).

PRIVACY (prof. Marchetti Spaccamela) (time: 60 mins)

4. Given the following table

Key	Quasi-Identifier			Sensitive
Name	*Sex*	*Age*	*Zip*	*Disease*
Alice	F	24	10000	Heart Disease
Bob	M	22	10000	Lung Cancer
Charlotte	F	24	10000	Breast Cancer
Dave	M	22	10000	Lung Cancer
Emma	F	20	10000	Heart Disease
Francis	M	20	10000	Heart Disease
Garry	M	22	10000	Lung Cancer
Harry	M	20	10000	Heart Disease
Iris	F	21	10001	Flu
John	F	21	10001	Flu
Kendra	F	20	10000	Heart Disease
Lisa	F	20	10000	Lung Cancer

k-Anonymity:

(i) Determine the largest k such that the table is k-anonym. Explain which rows contradict the (k+1)-anonymity.

(ii) You may now use suppression on the columns. Assume that by removing one digit from Age or Zip, or suppressing the Sex attribute, you lose one "value". What is the minimal value loss required to achieve 5-anonymity?

l-anonimity:

(iii) What is the largest l such that the above mentioned dataset is distinct l-diverse?
The dataset is distinct 1-diverse as QI = (F; 21; 10001) =) Disease = Flu.

(iv) Assume suppressing the last digit of the Zip column and generalising Age to {[0- 22]; [23-90]}
For what value of l can distinct l-diversity now be guaranteed.

5. What is differential privacy and discuss its advantages and disadvantages with respect ot other approaches. Provide one example in which differential privacy is useful.

6. Even when all nodes of Bitcoin are honest, blocks will occasionally get orphaned: if two miners Minnie and Mynie discover blocks nearly simultaneously, neither will have time to hear about the other's block before broadcasting hers.
   - What determines whose block will end up on the consensus branch?
   - What factors affect the rate of orphan blocks?
   - If Mynie hears about Minnie's block just before she's about to discover hers, does that mean she wasted her effort?