Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2016–2017, Semester: 2

Prof. G. Pelosi

February 2nd, 2018 – Exam Session

Name:.................................... Surname:..

Student ID:................................ Signature:...

Time: 2h:30'. Use of textbooks, notes, or Internet connected devices (including smartphones) is not allowed. The usage of simple calculators is allowed. Prior to turn in your paper, write your name on any additional sheet and sign it.

Question 1 [3 pts]

A file hosting service needs to have fixed-length unique `ID` for any file hosted.
The first proposal to compute an `ID` is to employ the digest provided by a SHA2-256 hash function. However, out of a concern for the induced overhead, the storage department proposes to

(i) employ a truncation of the aforementioned digests to 10 bytes or

(ii) alternatively, replace the SHA2-256 digest with the last block of a CBC-AES-256 encryption.

Argue for or against the said proposals, comparing the advantages and disadvantages of the three ways of computing the `ID` of a file.

Solution:
(sketch)
Truncation to 10 bytes of the digest provided by SHA2-256 hash function, reduces the chances to find a pair of inputs which collides on the same output value from $\approx 2^{128}$ down to $\approx 2^{40}$ (birthday paradox).
Replacing the SHA2-256 digest (256 refers to the digest size) with the last block of a CBC-AES-256 encryption (256 refers to the key size) also reduces the chances to find a pair of inputs which collides on the same output value from $\approx 2^{128}$ down to $\approx 2^{64}$ (birthday paradox).

Question 2 [2 pts]

Consider an OpenPGP certificate:

(a) Is it necessary for the owner of the primary public key contained in it, to sign the entire binary material in the certificate? Motivate your answer.

(b) Which parts of an OpenPGP certificate can be revoked by an OpenPGP user? How?

Solution:
(sketch)
The owner needs to certificate (via signature) the binding between her/his identity and the primary (public) key, as well as the binding between her/his primary key and the sub-keys (if any).
Signing the entire certificate content would prevent any other user from adding his signature to authenticate the owner's public key – without the certificate owner acknowledging it.

An OpenPGP user can revoke her/his own signature on the identity/primary-key binding signature or on the primary-key/subkey binding through appending a revocation signature to her/his own certificate. An OpenPGP user can revoke her/his own authenticating signature about the public-key/identity binding of another OpenPGP user through appending to the corresponding certificate a revocation signature.

Question 3 [3 pts]
Consider the Secure Shell cryptographic network protocol (SSH).
Describe how the remote server endpoint authentication is performed and what are the options to authenticate the user typing on the client.

Solution:
(sketch)
The remote server endpoint authentication is performed by the client via visual inspection of the public key fingerprint sent by the server (The server public key is not assumed to be signed by a CA, as the server simply transmits the public key value encoded in `base64` – not an entire X.509 certificate!).

The options to authenticate the user typing on the client are: password, user keypair (the client sign a challenge sent from the server with a private key associated to her), host keypair (the client sign a challenge sent from the server with a private key associated to client's machine), PAM (Pluggable Authentication Modules) – configurable authentication broker.

Question 4 [8 pts]

(a) Consider the cyclic group $(\mathbb{Z}^*_{5^4}, \cdot)$. Compute the cardinality of the group, the number of its generators and exhibit at least one generator for three of its proper subgroups.

(b) Consider the finite field $\mathbb{F}_{5^4}$. Find the number of irreducible and primitive polynomials. Determine **how** to check if $f(x){=}x^4+1{\in}\mathbb{F}_5[x]$ is a primitive polynomial.

Solution:

(a) $n{=}|(\mathbb{Z}^*_{5^4}, \cdot)|{=}\varphi(5^4){=}500{=}2^2 \cdot 5^3$

Number of generators: $\varphi(n){=}200$

Proper divisors of $n = 500 = 2^2 \cdot 5^3$: 2, 4, 5, 10, 20, 25, 50, 100, 125, 250
$g{=}2$ is a generator as the following powers are all distinct from 1

$g^2{\equiv}_{625}4, g^4{\equiv}_{625}16$, $g^5{\equiv}_{625}32$, $g^{10}{\equiv}_{625}399$,
$g^{20}{\equiv}_{625}399^2{\equiv}451$,
$g^{25}{\equiv}_{625}451 \cdot 32{\equiv}57$,
$g^{50}{\equiv}_{625}57^2{\equiv}124$,

$g^{100} \equiv_{625} 124^2 \equiv 376$,
$g^{125} \equiv_{625} 57^5 \equiv 182$,
$g^{250} \equiv_{625} 182^2 \equiv 624$

Three proper subgroups are the following ones:
$h_1 = g^{\frac{500}{2}} \equiv g^{250} \equiv_{625} -1$, $\quad |\langle h_1 \rangle| = 2$
$h_2 = g^{\frac{500}{5}} \equiv g^{100} \equiv_{625} 376$, $\quad |\langle h_2 \rangle| = 5$
$h_3 = g^{\frac{500}{10}} \equiv g^{50} \equiv_{625} 124$, $\quad |\langle h_3 \rangle| = 10$

(b) The number of irreducible polynomial of degree 4 can be derived from the following equality:
$N_4(5) \cdot 4 + N_2(5) \cdot 2 + N_1(5) \cdot 1 = 5^4$
$N_1(5) = 5$,
$N_2(5) = \frac{5^2-5}{2} = 10$,
$N_4(5) = \frac{5^4 - 10 \cdot 2 - 5 \cdot 1}{4} = 150$

The number of primitive polynomials of degree 4 is:
$M_4(5) = \frac{\varphi(5^4-1)}{4} = \frac{(2^4-2^3)\cdot(3^1-1)\cdot(13-1)\cdot}{4} = 48.$
Assuming $\alpha \in \mathbb{F}_{5^4} \setminus \mathbb{F}_5$ to be primitive and $f(\alpha)=0 \Leftrightarrow \alpha^4 \equiv_5 4$, as $|\alpha| = |\mathbb{F}^*_{5^4}| = 624 = 2^4 \cdot 3 \cdot 13$, then the proper divisors of 624 are:
$2, 3, 4, 6, 8, 12, 13, 16, 24, 26, 39, \ldots$.
We need to check if α is a generator, that is if
$\alpha^2 \not\equiv 1$ is true,
$\alpha^3 \not\equiv 1$ is true,
$\alpha^4 \not\equiv 1$ is true,
etc...

Question 5 [6 pts]

(a) Which are the criteria to select a suitable group, $(G, \cdot)$ $n = |G|$, for a discrete logarithm based cryptosystem?

(b) Consider the TLS handshake from ver. 1.1. After receiving the `Client_Hello` message (including the highest TLS ver. and the supported cipher-suite), the server will present its certificate sending back the `Server_Hello` message (including a nonce, its TLS ver. and a choice for the cipher-suite to employed). The client, will then check the received certificate and will send to the server a `Client_Key_Exchange` message including a 48byte randomly chosen pre-masker key – encrypted with the public key of the server. Both the client and the server will agree on a *master secret*, derived from the client's *pre-master secret* and the nonce chosen by the server. The client will sent also a `Change_Cipher_Spec` message, notifying that the communication will be encrypted and a `Finished` message including a MAC of all previous messages. The server will decrypt the `Finished` message, check the MAC and compose an encrypted response with identical content.
Note that the server key pair is used for two purposes: authentication of the server and encryption of a pre-master secret. Authentication only matters while the communication is established, but encryption is expected to last for years.

- What are the effects of a disclosure of the server's private key?
- How such effects can be mitigated? Which cipher-suite features are useful to be negotiated in this respect?

Solution:
(sketch)
The factors composing the group order must be sufficiently large to withstand a Poligh-Hellman attack, i.e., the smallest (prime) factor of the order must be at least 160-bit long.

The confidentiality of the past (...and future) communications is compromised as the adversary can recompute the session keys of his choice. Possible mitigations:

- set an expiration date in the server's certificate or force a periodic refresh of the key-material.
- enforce the Perfect Forward Secrecy agreeing on the pre master key via a Diffie-Hellman key exchange. The use of the Diffie-Hellman Ephemeral (DHE) key exchange can be negotiated among the cipher suite features.

Question 6 [12 pts]

(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 713$.
Assume $f(x) = x^2 + 1 \bmod n$ as the "random-walking" function.
Show every step of the computation.
(As a backup alternative, apply a "trivial division" strategy).

(b) Choose an admissible public exponent e between the values $e{=}3_{\texttt{dec}}$, $e{=}5_{\texttt{dec}}$, and $e{=}7_{\texttt{dec}}$ and compute the value of the corresponding RSA private key $k_{priv}{=}(p, q, \varphi(n), d)$. Show every step of the computation.

(c) Sign the message $m{=}5_{\texttt{dec}}{\in}\mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

(d) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_p, +, \times)$, $p{=}23$

- Show the definition of the Montgomery Multiplication and the smallest admissible value for the Montgomery Radix: R
- Show the high-level pseudo-code to implement the Montgomery Reduction procedure `MRed(...)`, and prove the correctness of the algorithm.
- Compute a pair of integer values R', p' that satisfy the relation: $\gcd(R, p){=}R{\cdot}R'{-}p{\cdot}p'{=}1$.
- Compute the Montgomery multiplication $C = A \times B \bmod p$, where $A = 17_{\text{dec}}$ and $B = 8_{\text{dec}}$ are values in the Montgomery domain, assuming a binary encoding of the operands

Solution:
(a) see lectures ... $q = 23$, $p = 31$
(b) $\varphi(n){=}22 \cdot 30{=}2^2 \cdot 3 \cdot 5 \cdot 11 = 660$, therefore the admissible value for the public exponent is $e{=}7_{\texttt{dec}}{\in}\mathbb{Z}^*_{\varphi(n)}$
$d{\equiv}_{\varphi(n)} e^{-1}{\equiv}_{660} 7^{-1}$
$\varphi(\varphi(n)) = \varphi(660) = (2^2 - 2) \cdot (3 - 1) \cdot (5 - 1) \cdot (11 - 1) = 160$
$d{\equiv}_{\varphi(n)} 7^{\varphi(\varphi(n))-1}{\equiv}_{660} 7^{159}{\equiv}7^{(10011111)_2}{\equiv}...{\equiv}283$

(c) $s{=}191_{\mathrm{dec}}$

(d) see lectures ... $R{=}32$, $\gcd(R,p) = \gcd(32,23) = 1 \Rightarrow 32 \cdot (-5) - 23 \cdot (-7) = 1$
$R' {\equiv_{23}} {-5} {\equiv_{23}} 18$, $p' {\equiv_{32}} {-7} {\equiv_{32}} 25$.
$C{=}\mathrm{MonPro}(17,8) {\equiv_{23}} 17{\cdot}8{\cdot}18 {\equiv_{23}} 10_{\mathrm{decimal}}$.