Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2018–2019, Semester: 2

Prof. G. Pelosi

July 2nd, 2019

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

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

Time: 2h, 15min. 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]
Consider an improved version of the Vigenère cipher, where instead of using multiple shift ciphers, multiple mono-alphabetic substitution ciphers are used. That is, the key consists of t random permutations of the alphabet, and the plaintext characters in positions i, $t+i$, $2t+i$, and so on, are encrypted using the ith permutation.
Show how to break this version of the cipher.

Solution:
The first point to note is that Kasiski's method for determining t works for this cipher as well. The only difference is therefore in the second stage of the attack. Here, one needs to build a frequency table for each of the t keys, and carry out an attack like on the mono-alphabetic cipher. Given a long enough plaintext, this will work successfully.

Question 2 [5 pts]
Consider a 128-bit block symmetric cipher, built with a Substitution-Permutation network approach. Two alternate designs are available, both employing a key addition via bitwise `xor`:

- Design A: 4×4 bit S-boxes, having a worst-case linear bias of $\frac{1}{8}$, and a worst case differential probability of $\frac{1}{4}$. Permutation layer built so that a single bit input to the permutation layer will affect four distinct S-Boxes on the next round.
- Design B: 8×8 bit S-Boxes, with worst-case linear bias of $\frac{1}{64}$ and worst-case differential probability of $\frac{1}{64}$. Permutation layer built so that a single bit input will affect two S-Boxes on the next round.

(a) What is the design that allows to build the shortest (in terms of number of rounds) block cipher, assuming a key length of 128 bits?

Solution:

(a) Design A will need to approximate 1 S-Box with two rounds, 5 with three rounds, 21 with four rounds, and 53 with five rounds. This results in the linear bias falling as $\frac{1}{8}, \frac{1}{2^{3\times5}}2^4 = 2^{-11}, \frac{1}{2^{3\times21}}2^{20} = 2^{-43}, \frac{1}{2^{3\times53}}2^{52} = 2^{-107}$. Since performing linear cryptanalysis requires $\frac{1}{bias^2}$ input-output pairs, a five round block cipher with design A will require more plaintext-ciphertext pairs than the one available (i.e., 2^{128}) to an attacker trying to exploit the four round linear bias of 2^{-107}. Concerning differential cryptanalysis, the differential probabilities will fall as: $\frac{1}{4}, \frac{1}{2^{2\times5}} = 2^{-10}, \frac{1}{2^{2\times21}} = 2^{-42}, \frac{1}{2^{2\times53}} = 2^{-106}$. Recalling that differential cryptanalysis needs $\frac{1}{p_{diff}}$ input-output pairs, the differential probability after five round will effectively be smaller than $\frac{1}{2^{128}}$. Therefore, since six rounds are needed to prevent an attacker from exploiting the differential probability at the fifth round due to the lack of input-output pairs.

Design B will need to approximate 1 S-Box with two rounds, 3 with three rounds, 7 with four rounds, 15 with five rounds, and 31 with six rounds. This results in the linear bias falling as $\frac{1}{64}, \frac{1}{2^{6\times3}}2^2 = 2^{-16}, \frac{1}{2^{6\times7}}2^6 = 2^{-36}, \frac{1}{2^{6\times15}}2^{14} = 2^{-76}, \frac{1}{2^{6\times31}}2^{30} = 2^{-156}$. Since performing linear cryptanalysis requires $\frac{1}{bias^2}$ input-output pairs, five rounds of design B are sufficient to be immune to it. Concerning differential cryptanalysis, the differential probabilities will fall as: $\frac{1}{64}, \frac{1}{2^{6\times3}} = 2^{-18}, \frac{1}{2^{6\times7}} = 2^{-42}, \frac{1}{2^{6\times15}} = 2^{-90}, \frac{1}{2^{6\times31}} = 2^{-186}$. Recalling that differential cryptanalysis needs $\frac{1}{p_{diff}}$ input-output pairs, six rounds are needed to achieve the desired immunity for design B.

As a consequence, both designs require six rounds to be immune to both linear and differential cryptanalysis.

Question 3 [3 pts]
Consider the case of connections employing the TLS protocol.

(a) What is the advantage of exploiting a TLS based secure transport to build a point-to-point VPN with respect to an IPSec based alternative?

(b) Is it possible to detect TLS connection downgrades to an unwanted version assuming that only the client configuration can be chosen at will?

(c) Is it possible to do the same assuming that only the server configuration can be chosen at will?

Solution:

(a) A TLS based point-to-point VPN will be able to work through Network Address and Port Translation (NAPT) services, while an IPSec based one will not, as the port number is kept within the encrypted payload.

(b) Only in TLS version 1.3 this is possible as the random nonce will be modified by a TLS 1.3 server receiving a mangled request for a downgraded connection in such a fashion that the client will be able to detect the downgrade attempt.

(c) Yes, in any TLS version it is the server which ultimately decides the TLS version to be employed. It is sufficient to configure a server in such a way that no versions below the ones acceptable are employed.

Extensive explanations on slides.

Question 4 [6 pts]

(a) List the cardinality, number of subgroups and number of generators of the following multiplicative groups: $(\mathbb{Z}_{49}, \times)$ and $(\mathbb{F}_{7^2}^*, \cdot)$.

(b) $f(x) = x^2 + x + 3 \in \mathbb{F}_7[x]$ is a primitive polynomial for $\mathbb{F}_{7^2}$. Show the roots of $f(x)$ as elements of $\mathbb{F}_{7^2} \cong \{\theta_6\alpha^6 + \theta_5\alpha^5 + \ldots + \theta_1\alpha + \theta_0,\ \theta_i \in \mathbb{F}_7, 0 \leq i \leq 6\ f(\alpha) = 0\}$.

(c) The DSS-DSA standard recommends a public key with two primes p, q such that the pair (L, N), with $L = \log_2(p)$ and $N = \log_2(q)$, is in the following list: (1024,160), (2048,224), (2048,256), and (3072,256).
What is the purpose of p, q in the public key?
What is the reason for including q in the public key?

Solution:

(a) $|\mathbb{Z}_{49}| = \varphi(7^2) = 7^2 - 7 = 42 = 2 \cdot 3 \cdot 7$.
The number of subgroups of $(\mathbb{Z}_{49}, \times)$ equals the number of divisors of its cardinality i.e.: $|\{1, 2, 3, 6, 7, 14, 21, 42\}| = 8$.
The number of generators of the cyclic group $(\mathbb{Z}_{49}, \times)$ is $\varphi(42) = (2-1)\cdot(3-1)\cdot(7-1) = 12$.

$|\mathbb{F}_{7^2}^*| = 7^2 - 1 = 48 = 2^4 \cdot 3$.
The number of subgroups of $(\mathbb{F}_{7^2}^*, \cdot)$ equals the number of divisors of its cardinality i.e.: $|\{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}| = 10$.
The number of generators of the cyclic group $(\mathbb{F}_{7^2}^*, \cdot)$ is $\varphi(48) = (2^4 - 2^3)\cdot(3-1) = 16$.

(b) $\alpha \in \mathbb{F}_{7^2} \setminus \mathbb{F}_7$, $f(\alpha) = 0$, $\alpha^2 \equiv -\alpha - 3$.
the two conjugate roots of f(x) are α and α^7, where $\alpha^7 \equiv (\alpha^2 \cdot \alpha)^2 \cdot \alpha \equiv$
$\equiv (-\alpha^2 - 3 \cdot \alpha)^2 \cdot \alpha \equiv (-2 \cdot \alpha + 3)^2 \cdot \alpha \equiv (4\alpha^2 + 2 + 2\alpha) \cdot \alpha \equiv (-2\alpha + 4) \cdot \alpha \equiv$
$6\alpha + 6 \equiv -\alpha - 1$.

(c) see lectures...

Question 5 [5 pts]
Consider the following relation: $13 \equiv 3^x \bmod 17$.

(a) Compute the discrete logarithm $x \equiv_{\varphi(17)} \log_3^{\mathrm{D}}(13)$ applying the Pohlig-Hellman method.

(b) Show the computational complexity of the Pohlig-Hellman algorithm. When is it appropriate to use this method?

Solution:

(a) We are considering the algebra of the group $(\mathbb{Z}_{17}^*, \cdot)$,
with $n = |\mathbb{Z}_{17}^*| = \varphi(17) = 16 = 2^4$ elements.

$$x \equiv_{\varphi(17)} \log_3^{\mathrm{D}}(13) \Leftrightarrow x \bmod 2^4 \equiv \log_3^{\mathrm{D}}(13) \bmod 2^4$$

The Pohlig-Hellman algorithm compute $(x \bmod p_1^4)$, with $p_1 = 2$, as follows:
let the 2-radix expansion of $x \bmod 2^4$ be $x = l_0 + l_1 \cdot p_1 + l_2 \cdot p_1^2 + l_3 \cdot p_1^3$ and denote as: $g = 3$ the base of the logarithm, $\beta = 13$, $n = 16$ the order of the group.

$\eta = g^{\frac{n}{p_1}} \equiv_{17} 3^8 \equiv_{17} 16 \equiv_{17} -1.$

$\gamma_0 = 1,$
$\delta_0 \equiv (\beta\gamma_0^{-1})^{\frac{n}{p_1}} \equiv_{17} 13^8 \equiv_{17} 1.$
Knowing that $\delta_0 = (g^x\gamma_0^{-1})^{\frac{n}{p_1}} \equiv (g^{l_0+l_1\cdot p_1+l_2\cdot p_1^2+l_3\cdot p_1^3})^{\frac{n}{p_1}} \Rightarrow \delta_0 \equiv (g^{\frac{n}{p_1}})^{l_0} \Leftrightarrow \delta_0 \equiv \eta^{l_0}$,
$1 \equiv_{17} (-1)^{l_0}$, therefore: $l_0 = 0$.

$\gamma_1 = \gamma_0 \cdot g^{l_0 p_1^0} \equiv_{17} 1,$
$\delta_1 \equiv (\beta\gamma_1^{-1})^{\frac{n}{p_1^2}} \equiv_{17} 13^4 \equiv_{17} 1.$
Knowing that $\delta_1 = (g^x\gamma_1^{-1})^{\frac{n}{p_1^2}} \equiv (g^{x-l_0})^{\frac{n}{p_1^2}} \Rightarrow \delta_1 \equiv (g^{\frac{n}{p_1}})^{l_1} \Leftrightarrow \delta_1 \equiv \eta^{l_1}$,
$1 \equiv_{17} (-1)^{l_1}$, therefore: $l_1 = 0$.

$\gamma_2 = \gamma_1 \cdot g^{l_0 p_1^0 + l_1 p_1^1} \equiv_{17} 1,$
$\delta_2 \equiv (\beta\gamma_2^{-1})^{\frac{n}{p_1^3}} \equiv_{17} 13^2 \equiv_{17} 16 \equiv_{17} -1.$
Knowing that $\delta_2 = (g^x\gamma_2^{-1})^{\frac{n}{p_1^3}} \equiv (g^{x-l_0-l_1 p_1})^{\frac{n}{p_1^3}} \Rightarrow \delta_2 \equiv (g^{\frac{n}{p_1}})^{l_2} \Leftrightarrow \delta_2 \equiv \eta^{l_2}$,
$-1 \equiv_{17} (-1)^{l_2}$, therefore: $l_2 = 1$.

$\gamma_3 = \gamma_2 \cdot g^{l_0 p_1^0 + l_1 p_1^1 + l_2 p_1^2} \equiv_{17} 3^4 \equiv_{17} 13,$
$\delta_3 \equiv (\beta\gamma_3^{-1})^{\frac{n}{p_1^4}} \equiv_{17} 13 \cdot 13^{-1} \equiv_{17} 1.$
Knowing that $\delta_3 = (g^x\gamma_3^{-1})^{\frac{n}{p_1^4}} \equiv (g^{x_1-l_0})^{\frac{n}{p_1^4}} \Rightarrow \delta_3 \equiv (g^{\frac{n}{p_1}})^{l_3} \Leftrightarrow \delta_3 \equiv \eta^{l_3}$,
$1 \equiv_{17} (-1)^{l_3}$, therefore: $l_3 = 0$.

$x = l_0 + l_1 \cdot 2 + l_2 \cdot 2^2 + l_3 \cdot 2^3 = 2^2 = 4.$
Validation: $3^x \stackrel{?}{\equiv}_{17} 13$, taking x=4, it is true that $3^4 \equiv_{17} 13$.

(b) (see lectures...)

Question 6 [12 pts]

(a) Describe the Fermat primality test and the Miller-Rabin primality test.

(b) Apply the Pollard's ρ method[1] to factor the RSA public modulus $n = p \cdot q = 1357$

(c) Given the factorization of $n = p \cdot q$, note that $p = 2p_1 + 1$ and $q = 2q_1 + 1$, with p_1 and q_1 also prime numbers. Show the number of possible values for the RSA encryption exponent e as a function of p_1 and q_1 and compute its value. Subsequently, assuming $e = 5$, compute the corresponding RSA private key, justifying your answer.

(d) Assume that a smart-card contains an RSA co-processor with an hardcoded public modulus $n = 1541$, and a school-book implementation (no OAEP), leaving the choice of the public exponent to the user. Eve obtains two encryptions of the same message m with the following

[1] as a back-up strategy you can apply a trivial division method

two public exponents: $e_A = 5$, $e_B = 7$.
Can she derive the plaintext message?
Motivate your answer and show every step of the computation.

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

- Exhibit the smallest admissible value for the Montgomery Radix, R, and the values R', p' that satisfy the relation: $\gcd(R, p) = R\,R' - p\,p' = 1$, justifying your answer;
- Compute the Montgomery multiplication $\widetilde{C} = \text{MonPro}(\widetilde{A}, \widetilde{B}) = \widetilde{A} \cdot \widetilde{B} \cdot R^{-1} \bmod p$, where $\widetilde{A} = 16_{\text{dec}}$ and $\widetilde{B} = 11_{\text{dec}}$, assuming a binary encoding of the operands.

Solution:
(Sketch)

(e) $R = 2^5 = 32$. $\gcd(32, 23) = 32(-5) - 23(-7) = 1 \Rightarrow$
$R' = R^{-1} \bmod p \equiv_{23} -5 \equiv_{23} 18$, $p' = p^{-1} \bmod R \equiv_{32} -7 \equiv_{32} 25$.

$p = 23_{\text{dec}} = \langle 10111 \rangle_2, \qquad p'_0 = (p' \bmod 2) = 1$
$\widetilde{B} = 11_{\text{dec}} = \langle \widetilde{B}_4 \widetilde{B}_3 \widetilde{B}_2 \widetilde{B}_1 \widetilde{B}_0 \rangle_2 = \langle 01011 \rangle_2$
$\widetilde{A} = 16_{\text{dec}} = \langle \widetilde{A}_4 \widetilde{A}_3 \widetilde{A}_2 \widetilde{A}_1 \widetilde{A}_0 \rangle_2 = \langle 10000 \rangle_2$

00000	+
00000	$\widetilde{A}_0 \widetilde{B} = \langle 00000 \rangle_2$
00000	+
00000	$(p'_0 x_0)\, p = \langle 00000 \rangle_2$
00000	perform a right-shift of 1 bit
⋮	⋮
00000	+
01011	$\widetilde{A}_4 \widetilde{B} = \langle 01011 \rangle_2$
01011	+
10111	$(p'_0 x_0)\, p = \langle 10111 \rangle_2$
100010	perform a right-shift of 1 bit
10001	

$\widetilde{C} = \langle 10001 \rangle_2 = 17_{\text{dec}} < \mathbf{p}$, Thus: $C \equiv_p \text{MonPro}(16_{\text{dec}}, 11_{\text{dec}}) \equiv_{23} 17_{\text{dec}}$

Validation:

$\widetilde{C} = \text{MonPro}(16, 11) \stackrel{\text{def}}{=} 16 \cdot 11 \cdot R^{-1} \bmod p \equiv_{23} 15 \cdot 32^{-1} \equiv_{23} 15 \cdot 18 \equiv_{23} 17_{\text{dec}}$