Exercise 10 in Cryptography - Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-07-09

Solution of Problem 32

MITM attack can be easily avoided if:

given $p = 2q + 1$, p and q prime $\Longrightarrow$

$\Longrightarrow a^q = a^{\frac{p-1}{2}}$ has order 2, since $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1$ using Fermat theorem.

Now using the scheme of DH key-exchange:

$$\begin{matrix} \text{A} \xrightarrow{a^x} \text{O} \xrightarrow{a^{xq}} \text{B} \\ \text{A} \xleftarrow{a^{yq}} \text{O} \xleftarrow{a^y} \text{B} \end{matrix} \Longrightarrow \text{common key: } a^{xyq} = (a^q)^{xy}$$

$$a^q \text{ has order } 2 \Longrightarrow a^q \in \{-1, 1\} \Longrightarrow a^{qxy} \in \{-1, 1\}.$$

Therefore, as a counter measure, we just need to check if:

$$\text{key} = \pm 1$$

Solution of Problem 33

Shamir's no-key protocol with the parameters: $p = 31337, a = 9999, b = 1011, m = 3567$.

a)

$$c_1 = m^a \mod p = 3567^{9999} \mod 31337 \equiv 6399 \quad (1)$$

$$c_2 = c_1^b \mod p = 6399^{1011} \mod 31337 \equiv 29872 \text{ (given by hint)} \quad (2)$$

$$c_3 = c_2^{a^{-1}} \mod p = 29872^{14767} \mod 31337 \equiv 24982 \quad (3)$$

To compute c_1 we use the square-and-multiply algorithm (SAM) (in chart):

The binary representation of $a = 9999$ is 10011100001111_2.

Hint: If your calculator can not convert a large number $\Rightarrow$ convert it by hand.

For illustration, we can represent the exponentiation in terms of squareings by:

$$m^a \equiv (\ldots(m^1)^2 m^0)^2 m^0)^2 m^1)^2 m^1)^2 m^1)^2 m^0)^2 m^0)^2 m^0)^2 m^0)^2 m^1)^2 m^1)^2 m^1)^2 m^1 \mod p$$

op	exp	modulo
1	1	3567
S	0	667
S	0	6171
SM	1	13498
SM	1	23177
SM	1	3298
S	0	2865
S	0	29268
S	0	18929
S	0	31120
SM	1	143
SM	1	20384
SM	1	30182
SM	1	6399

Hint: Feel free to implement the SAM in order to check your results.

To compute a^{-1} modulo $p-1$, we use the EEA:

$$\begin{aligned}
31336 &= 3 \cdot 9999 + 1339 \\
9999 &= 7 \cdot 1339 + 626 \\
1339 &= 2 \cdot 626 + 87 \\
626 &= 7 \cdot 87 + 17 \\
87 &= 5 \cdot 17 + 2 \\
17 &= 8 \cdot 2 + 1 \Rightarrow \gcd(31336, 9999) = 1
\end{aligned}$$

To compute the inverse of a, we reorganize the last equation w.r.t. the remainder one and substitute the factors backwards:

$$\begin{aligned}
1 &= 17 - 8 \cdot 2 \\
&= 17 - 8 \cdot (87 - 5 \cdot 17) = 41 \cdot 17 - 8 \cdot 87 \\
&= 41 \cdot 626 - 295 \cdot 87 \\
&= 631 \cdot 626 - 295 \cdot 1339 \\
&= 631 \cdot 9999 - 4712 \cdot 1339 \\
&= \underbrace{14767}_{a^{-1}} \cdot \underbrace{9999}_{a} - 4712 \cdot 31336
\end{aligned}$$

Hint: Check if result is equal to one in each step!

The computation of $c_2^{a^{-1}} \mod p = 29872^{14767} \mod 31337$ with SAM provides:

op	exp	modulo
1	1	29872
SM	1	9607
SM	1	15639
S	0	24373
S	0	18957
SM	1	16656
SM	1	26421
S	0	6229
SM	1	8290
S	0	2059
SM	1	28387
SM	1	13917
SM	1	9317
SM	1	24982

Solution of Problem 34

a) The public parameters and the received ciphertext are:

- $e = d^{-1} \mod \varphi(n)$,
- $n = p\,q$,
- $c = m^e \mod n$.

The plaintext m is not relatively prime to n , i.e., $p \mid m$ or $q \mid m$ and $p \neq q$.

Hence, $\gcd(m, n) \in \{p, q\}$ holds. The $\gcd(m, n)$ can be easily computed such that both primes can be calculated by either $q = \frac{n}{p}$ or $p = \frac{n}{q}$.

The private key d can be computed since the factorization of $n = p\,q$ is known.

$$d = e^{-1} \mod \varphi(p\,q) = e^{-1} \mod (p-1)(q-1).$$

This inverse is computed using the extended Euclidean algorithm.

b) m, n have common divisors.

The number of relatively prime numbers to n are $\varphi(n) = (p-1)(q-1) = p\,q-(p+q)+1$.

$$\mathrm{P}(\gcd(m, n) = 1) = \frac{\varphi(n)}{n-1}.$$

The complementary probability is computed by:

$$\begin{aligned} P = \mathrm{P}(\gcd(m, n) \neq 1) = 1 - \frac{\varphi(n)}{n-1} &= \frac{n-1-\varphi(n)}{n-1} \\ &= \frac{p\,q - p\,q + p + q - 2}{p\,q - 1} = \frac{p+q-2}{p\,q-1}. \end{aligned}$$

c) $n : 1024$ Bits $\Rightarrow p \approx \sqrt{n} = 2^{512}, q \approx \sqrt{n} = 2^{512}$. From (b) we compute:

$$P = \frac{2^{512} + 2^{512} - 2}{2^{1024} - 1} = \frac{2^{513} - 2}{2^{1024} - 1} \approx 2^{-511} = (2^{-10})^{51} 2^{-1} \approx (10^{-3})^{51} \frac{5}{10} = 5 \cdot 10^{-154}$$

In general: $n = 2^k$, $p, q \approx 2^{\frac{k}{2}}$ for k Bits.

$$P = \frac{2^{\frac{k}{2}} + 2^{\frac{k}{2}} - 2}{2^k - 1} = \frac{2^{\frac{k}{2}+1} - 2}{2^k - 1} \approx 2^{\frac{k}{2}+1} 2^{-k} = 2^{-\frac{k}{2}+1}.$$

Thus, the probability that m and n are coprime is marginal, if n has sufficiently many bits.

Solution of Problem 35

Let $n = p \cdot q$, $p \neq q$ be prime and x a non-trivial solution of $x^2 \equiv 1 \ (mod\ n)$, i.e., $x \not\equiv \pm 1 \ (mod\ n)$. Then:

$$\gcd(x+1, n) \in \{p, q\}$$

Proof:

$$\begin{aligned} x^2 \equiv 1 \ (mod\ n) &\iff (x^2 - 1) \equiv 0 \ (mod\ n) \\ &\iff (x+1)(x-1) \equiv 0 \ (mod\ n) \\ &\iff (x+1)(x-1) = k \cdot p \cdot q \quad \exists k \in \mathbb{N} \end{aligned}$$

$$\begin{aligned} &\iff p \cdot q \ |(x+1)(x-1) \\ &\iff p \text{ divides either } (x+1) \text{ or } (x-1) \\ &\iff q \text{ divides either } (x+1) \text{ or } (x-1) \end{aligned}$$

and $x - 1 < x + 1 < n$ holds:

$$\left.\begin{aligned} &\iff p \cdot q \nmid (x+1) \iff p \cdot q > x+1 \\ &\iff p \cdot q \nmid (x-1) \iff p \cdot q > x-1 \end{aligned}\right\} \implies gcd(x+1, n) \neq p \cdot q = n$$

$\iff$ either p or q divide $x + 1 \implies \gcd(x+1, n) \in \{p, q\}$ ✓