«به نام خدا»

تکلیف ششم – مرضیه علیدادی – 9631983
(سوال های 1 تا 4)

1.

a) n = $\frac{1}{2} + \sqrt{\frac{1}{4} + 2 * \ln(2) * 365} = 22.999 \approx 23$

b) p(at least two students) = $1 - \prod_{i=1}^{k-1} (1 - \frac{i}{N})$

c) t = $2^{n+1/2} \sqrt{\ln\left(\frac{1}{1-\lambda}\right)} = 2^{n+1/2} \sqrt{\ln\left(\frac{1}{1-0.5}\right)} = 2^{n+1/2} \sqrt{\ln(2)} = 0.83 * 2^{n+1/2}$

2.

from this formula of birth-date problem: k $\approx \sqrt{n * m * \frac{1}{1-\varepsilon}}$

we got:

n	ε = 0.5	ε = 0.1
2^{64}	$3.6 * 10^9$	$1.4 * 10^9$
2^{128}	$1.5 * 10^{19}$	$6 * 10^{18}$
2^{160}	$1.5 * 10^{24}$	$3.9 * 10^{23}$

3.

3.1. $c_i = z_i \oplus \{x_1x_2 \ldots x_n \,||\, H_1(x)H_2(x) \ldots H_m(x)\}$; $(i = 1, 2, \ldots, n + m)$

assume the length of x is n.

the attacker computes: $z_i = x_i \oplus c_i$ $(i = 1, 2, \ldots, n)$

and computes H(x) because he has x.

again computes: $z_{j+n} = H_j(x) \oplus c_{j+n}$ $(j = 1, 2, \ldots, m)$

He computes H(x')

Then computes: $c'_i = z_i \oplus x'_i$ $(i = 1, 2, \ldots, n)$

$c'_{j+n} = z_{j+n} \oplus H_j(x')$ $(j = 1, 2, \ldots, m)$

3.2. No.

The attacker can still recover $z_1, z_2, \ldots, z_n$.

But he can't recover the bit-stream portion $z_{n+1}, z_{n+2}, \ldots, z_{n+m}$ which was used for encrypting $MAC_{k2}(x)$.

Even if he would know the whole bit-stream, he wouldn't be able to compute a valid $MAC_{k2}(x')$, since he doesn't know k_2.

4.

4.1. $t = 10^6$ bits/sec
storage = t * r = 2h * 10^6 bits/sec = 2 * 3600 * 10^6 bits/sec = 7.2 Gbits = 0.9 GByte
Storage of less than 1 GByte can be done at moderate costs, e.g., on hard disks or CDs.

4.2. We should first Compute the number of keys that an attacker can recover in 30 days:

Number of keys = $\frac{30 \text{ days}}{10 \text{ mins}} = \frac{30*24*60}{10}$ = 4320
Key derivation period = $\frac{2 \text{ h}}{4320}$ = 1.67 sec
Because has functions are fast, a key derivation can easily be performed (in software) at such a rate.