INGI2347 : Exercises
Lecture 6 *

Xavier Carpent

March 9, 2015

Solution 1: Symmetric Encryption Modes (continued)

1. The birthday paradox indicates that after having observed 2^{32} data blocks (which corresponds to 32 GB of encrypted data in the case of Triple-DES), the probability of observing a collision is approximately equal to 40%. This explains why the successor of DES, the AES algorithm, has a block size of 128 bits: in this case, it would be necessary to observe 2^{64} blocks of 128 bits to obtain the same success probability, which is unrealistic with the current technology.

Solution 2: Hash Functions and the Birthday Paradox

This exercise illustrates the *birthday paradox*: what is the probability that, in a group, at least two people have the same birthday? The probability that at least two people in a group of 23 people have the same birthday is higher than 0.5, which is much higher than our intuition would suggest, hence the term paradox.

1. Let p be the probability that at least one person has a certificate having the same signature as Gérard Mansoiffe and $\bar{p}$ the complementary probability, i.e., the probability that nobody has a certificate having the same signature as Gérard's. Let H be the number of possible fingerprints (2^{160}), and N be the number of people on Earth. The probability that one particular person has the same signature as Gérard is $\frac{1}{H}$; the probability that it has different is thus $1 - \frac{1}{H}$. There are $N - 1$ other people. Thus we deduce p as:

$$p = 1 - \bar{p} = 1 - \left(1 - \frac{1}{H}\right)^{N-1} = 1 - \left(1 - \frac{1}{2^{160}}\right)^{6\times 10^9 - 1}$$

We obtain a good approximation using twice the fact that $1 - x \approx e^{-x}$, for x close to 0.

$$p \approx 1 - e^{\frac{-(N-1)}{H}} \approx \frac{N-1}{H} \approx 4.1 \times 10^{-39}$$

2. Assume now that p' is the probability that at least two people on Earth have certificates with the same signature. Let $\bar{p'}$ be the complementary probability i.e., probability that all people on the Earth have distinct fingerprints. To calculate $\bar{p'}$ let us think of a table containing H cells. Each of the N people comes to cross out the cell corresponding to their signature. The first cross inevitably falls on a free cell. For the second, there is $\frac{H-1}{H}$ chances that it falls on a free cell. For the third $\frac{H-2}{H}$, and so on. Thus we have:

$$p' = 1 - \bar{p'} = 1 - \left(\frac{H-1}{H}\right)\left(\frac{H-2}{H}\right)\dots\left(\frac{H-(N-1)}{H}\right) = 1 - \prod_{i=1}^{N-1}\left(1 - \frac{i}{H}\right)$$

thus

$$p' \approx 1 - e^{\frac{-N(N-1)}{2\times H}} \approx \frac{N(N-1)}{2\times H} \approx 1.2 \times 10^{-29}$$

Solution 3: RSA Algorithm

1. To generate a pair (public key, private key), the following procedure must be applied:
   - generate two large prime numbers p and q;
   - calculate $n := pq$ et $\phi(n) = (p-1)(q-1)$;
   - choose e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$;
   - calculate d such that $ed \equiv 1 \bmod \phi(n)$;
   - publish (e, n) and keep (d, n) private (or, in an equivalent manner, the (d, p, q) triplet).

2. The encrypted message is $16^{17} \bmod 55$. Using the fact that $16^5 \equiv 1 \pmod{55}$, we easily find that $16^{17} \equiv 16^2 \equiv 256 \equiv 36 \pmod{55}$.

3. We can obtain $8^{33} \equiv ((((((8)^2)^2)^2)^2)^2) * 8 \equiv 28 \bmod 55$ using the "square and multiply" algorithm.

4. The encrypted message length must be lower than n. Since the decrypting message is computed " $\pmod{55}$", it would be impossible to recover the initial message if it is greater than 54.

5. Such messages are typically hashed before being signed.

Solution 4: RSA Vulnerabilities

Let s_1 (resp. s_2) be the signature of message m_1 (resp. m_2) using the private key (d, n). Assume now s as the signature of the message $m = m_1 \times m_2$. We have :

$$\begin{aligned} s_1 \times s_2 &\equiv \left(m_1^d \bmod n\right)\left(m_2^d \bmod n\right) \\ &\equiv (m_1 m_2)^d \\ &= s \pmod{n} \end{aligned}$$

This proves that the product of the signatures of two messages (constructed using the same private key) is equal to the signature of the product of the two messages.

Solution 5: Exhaustive Search for Asymmetric Keys

In the worst case, the cryptanalyst would have to try all the prime numbers inferior to $\sqrt{2^{1024}} = 2^{512}$, of which there are approximately:

$$\pi\left(2^{512}\right) \approx \frac{2^{512}}{512 \ln 2} \approx 2^{503}$$

This attack is thus completely unrealistic. Better attacks exist, though (through modulus factorization, i.e. determining p and q). In 2006, one estimated that the best known algorithms associated to these dedicated machines would need the same computing time to factorize a 1024 bits RSA key as to break a 80 bits symmetric key.

Solution 6: Authenticated Encryption and Compression

1. There are several possibilities, but the three most relevant are:

- Encrypt-then-MAC (EtM): $MAC_{k_M}(E_{k_E}(m)), E_{k_E}(m)$
- MAC-then-Encrypt (MtE): $E_{k_E}(MAC_{k_M}(m), m)$
- Encrypt-and-MAC (EaM): $MAC_{k_M}(m), E_{k_E}(m)$

On a side note, one should normally use different keys k_E and k_M for encryption and MAC. This is a conservative approach.
2. Compression should be done before encryption. If encryption is done first, it results in a ciphertext which entropy is high (random-oracle property of ciphers), and will result in no visible compression. Moreover, if some form of lossy compression is used, compressing the ciphertext will make it undecipherable.