# HWSec: exam

Renaud Pacalet

26 June 2018

You can use any document you need. Please number the different pages of your work and indicate on each page your first and last names. Write your answers in French or in English, as you wish, but avoid mixing the languages. If some extra information or hypotheses are missing to answer a question or solve a problem, decide by yourself and write down the added hypotheses or information. If you consider a question as absurd and thus decide not to answer, explain why. If you do not have time to answer a question or solve a problem but know how to, briefly explain your ideas.

Important advice #1: quickly go through the document and answer first the easy parts.

Important advice #2: copying verbatim the slides of the lectures or any other provided material is not considered a valid answer.

The first part is a set of five questions (2 points each) and the second part is a small problem (10 points).

## 1 Questions

1.1. Side channel attacks: is it easier to protect a crypto-system against timing attacks or against power attacks. Why? Give an example of countermeasure against each of these two classes of attacks.

1.2. Timing attacks: the course enumerates 5 different hypothesis for a timing attack to be practical against the modular exponentiation $z = y^x \bmod n$:

- The cryptosystem takes slightly different amounts of time to process different inputs.
- Timing depends on encryption key $(x, n)$ and input data $y$.
- The attacker knows the input data $y$.
- For several input data $y$ the victim computes the ciphertext $y^x \bmod n$ and the attacker records the timing.
- The attacker knows the implementation and uses this knowledge to exploit the timing measurements.

For each of them propose a countermeasure based on nullifying it and discuss the efficiency of such a solution.

1.3. Power attacks: what are the main improvements that you can imagine to Paul Kocher's initial proposal for Differential Power Analysis (DPA) attacks?

1.4. Fault attacks: explain why "check before sending results" is not always sufficient to protect a system against fault attacks.

1.5. Where does it come from that fault attacks frequently require only a few experiments while side channel attacks require many?

## 2 La Blaisine and Cardinal de Richelieu

The 18th of October 1640 Pierre de Fermat wrote a letter to his friend Bernard Frénicle de Bessy in which he stated what is known today as Fermat's little theorem. The last pages of this letter have been lost and nobody knows what the very long and detailed post scriptum was. Fortunately, in a second-hand trade, I recently discovered Frénicle de Bessy's answer and I can reveal what the missing part was about: more than three-hundred years before Ron Rivest, Adi Shamir, and Leonard Adleman, Fermat invented public key cryptography and RSA!

Algorithm 1 shows the pseudo-code of Fermat's decryption algorithm. $C$ is the ciphertext, $M$ is the plain text, $N$ is the public modulus, $w$ is the bit-width of the secret exponent, $D$ is the $w$-bits secret exponent, $k$ is a loop index, $X$, $Y$ and the $T_k$ are temporary variables. The bits of $D$ are numbered from $D(w-1)$ (most significant) to $D(0)$ (least significant). For obvious security reasons Fermat recommended that $w$ should be chosen large (several hundreds or even thousands).

Figure 1: Pierre de Fermat

**Algorithm 1** Decryption

```
$T_w \Leftarrow 1$
$k \Leftarrow w - 1$
while $k \geq 0$ do
  $X \Leftarrow (T_{k+1})^2 \bmod N$
  $Y \Leftarrow (X \times C) \bmod N$
  if $D(k) = 0$ then
    $T_k \Leftarrow X$
  else
    $T_k \Leftarrow Y$
  end if
  $k \Leftarrow k - 1$
end while
return $T_0 = C^D \bmod N = M$
```

Figure 2: Blaise Pascal

As computers were not invented yet, Fermat asked Blaise Pascal to adapt one of his famous mechanical calculating machines to speed-up the computation of modular exponentiations. The machine Pascal designed, which he named *La Blaisine*, had hundreds of two-positions sliders for the input of the $N$, $D$ and $M$ parameters and for the output of the $C$ result, plus thousands of gears for the computation. It supported values of $w$ up to 4096. The Blaisine was computing one iteration of the algorithm each time the operator was rotating a big side handle (not represented on figure 3). Of course, it was extremely noisy.

One year later, in 1641, the members of the comte de Soissons' conspiracy against Cardinal de Richelieu decided to use the Blaisine to communicate securely. As the risk was enormous, they decided to use the largest possible value for $w$: 4096. Unfortunately for the conspirators, Richelieu had a spy, Milady de Winter, in the hostel where their secret messages were brought by a messenger and decrypted. Milady bribed the messenger with a purse of gold coins and got perfect copies of the ciphertexts. Each time a ciphertext was received, she also carefully listened to the decryption noise through the thin room wall. Her hearing was so sharp that, for each ciphertext, she could estimate with a good accuracy the **total** Hamming weight $H = \sum_{k=0}^{k=w-1} \text{HammingWeight}(T_k)$.

She **couldn't discover anything else** from the noise but it was apparently sufficient: after enough ciphertexts were received, Milady recovered the secret exponent $D$, decrypted all ciphertexts and the conspirators were arrested. Richelieu ordered the destruction of all Blaisines. Fermat and his friends wisely decided to work on less dangerous topics and it took about 330 years before the same ideas re-emerged.

Figure 3: La Blaisine (simplified scale model)

**TODO (6 points)**: Explain how Milady recovered the secret exponent $D$. Clearly define your notations and write the pseudo-code of the attack algorithm. Explain every detail.

**TODO (4 points)**: List all hypotheses that had to hold for Milady's attack to work. For each hypothesis explain how it could be cancelled, if it can, decide if this constitutes a viable countermeasure, discuss the advantages and drawbacks.