Sketch of Lecture 10

Wed, 2/5/2020

Sad but important lessons

Review. CSS (content scramble system) is based on 2 LFSRs whose outputs are added with carry (the carry is important because it combines the LFSRs in a nonlinear way).

Combining LFSRs in a nonlinear fashion is a good idea for constructing PRGs for cryptographic purposes (especially because they are simple to implement in hardware). However, as the examples of CSS as well as GSM/Bluetooth encryption show, a lot of attention has to be paid to the details in order not to compromise security.

CSS (and many other examples in recent history) teach us one important lesson:

Do not implement your own ideas for serious crypto!

We will soon see that there exist cryptosystems which are believed to be secure. While none of these beliefs are proven, we do know that certain of these are in fact secure (if implemented correctly) if and only if a certain important mathematical problem cannot be easily solved.

- So, to crack such a system, one has to solve a mathematical problem that many people care about deeply. If this happens, you will most likely read about it in the (academic) news, and you will have an opportunity to update your system in time (most likely, you'll hear about progress much earlier).
- On the other hand, if you use a cryptosystem that is not well-studied, then it may well happen that an adversary breaks your system and keeps exploiting the security leak without you ever learning about it.

Not particularly related but important to keep in mind:

Frequently, security's weakest link are humans. It's very hard to protect against that.

https://en.wikipedia.org/wiki/Social_engineering_(security)

Review: Chinese remainder theorem

Example 65. (warmup)

(a) If $x \equiv 3 \pmod{10}$, what can we say about $x \pmod{5}$?

(b) If $x \equiv 3 \pmod{7}$, what can we say about $x \pmod{5}$?

Solution.

(a) If $x \equiv 3 \pmod{10}$, then $x \equiv 3 \pmod{5}$.
[Why?! Because $x \equiv 3 \pmod{10}$ if and only if $x = 3 + 10m$, which modulo 5 reduces to $x \equiv 3 \pmod{5}$.]

(b) Absolutely nothing! $x = 3 + 7m$ can be anything modulo 5 (because $7 \equiv 2$ is invertible modulo 5).

Example 66. If $x \equiv 32 \pmod{35}$, then $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Why?! As in the first part of the warmup, if $x \equiv 32 \pmod{35}$, then $x \equiv 32 \pmod{5}$ and $x \equiv 32 \pmod{7}$.

The Chinese remainder theorem says that this can be reversed!

That is, if $x \equiv 2 \pmod{5}$ and $x \equiv 4 \pmod{7}$, then the value of x modulo $5 \cdot 7 = 35$ is determined.
[How to find the exact $x \equiv 32 \pmod{35}$ is discussed in the next example.]

Example 67. Solve $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$.

Solution. $x \equiv 2 \cdot 7 \cdot \underbrace{7_{\bmod 5}^{-1}}_{3} + 4 \cdot 5 \cdot \underbrace{5_{\bmod 7}^{-1}}_{3} \equiv 42 + 60 \equiv 32 \pmod{35}$

Important comment. Can you see how we need 5 and 7 to be coprime here?

Brute force solution. Note that, while in principle we can always perform a brute force search, this is not practical for larger problems. Here, if x is a solution, then so is $x + 35$. So we only look for solutions modulo 35.

Since $x \equiv 4 \pmod{7}$, the only candidates for solutions are $4, 11, 18, \ldots$ Among these, we find $x = 32$.

[We can also focus on $x \equiv 2 \pmod{5}$ and consider the candidates $2, 7, 12, \ldots$, but that is even more work.]

Example 68. (extra) Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 4 \pmod{7}$

Solution. $x \equiv 1 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)_{\bmod 3}^{-1}]}_{-1} + 2 \cdot 3 \cdot 7 \cdot \underbrace{[(3 \cdot 7)_{\bmod 5}^{-1}]}_{1} + 4 \cdot 3 \cdot 5 \cdot \underbrace{[(3 \cdot 5)_{\bmod 7}^{-1}]}_{1} \equiv 67 \pmod{105}$

Note. Comparing with the previous example, note that $67 \equiv 32 \pmod{35}$.

Theorem 69. (Chinese Remainder Theorem) Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad \ldots, \quad x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$.

In other words. The Chinese remainder theorem provides a bijective (i.e., 1-1 and onto) correspondence

$$x \pmod{nm} \mapsto \left[\begin{array}{c} x \pmod{n} \\ x \pmod{m} \end{array}\right]$$

provided that m and n are coprime.

For instance. Let's make the correspondence explicit for $n = 2$, $m = 3$:

$0 \mapsto \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $1 \mapsto \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$, $2 \mapsto \left[\begin{smallmatrix} 0 \\ 2 \end{smallmatrix}\right]$, $3 \mapsto \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $4 \mapsto \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$, $5 \mapsto \left[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right]$