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 66. (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 67. 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.]

Armin Straub
straub@southalabama.edu

Example 68. Solve $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$.

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

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 69. (extra) Solve $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$

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

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

Theorem 70. (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

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod n \\ x \pmod m \end{bmatrix}$$

provided that m and n are coprime.

For instance. Let's make the correspondence explicit for $n = 2$, $m = 3$:
$0 \mapsto \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $1 \mapsto \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $2 \mapsto \begin{bmatrix} 0 \\ 2 \end{bmatrix}$, $3 \mapsto \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $4 \mapsto \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $5 \mapsto \begin{bmatrix} 1 \\ 2 \end{bmatrix}$

Example 71. Solve $x \equiv 4 \pmod 5$, $x \equiv 10 \pmod{13}$.

Solution. $x \equiv 4 \cdot 13 \cdot \underbrace{13^{-1}_{\bmod 5}}_{2} + 10 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 13}}_{-5} \equiv 104 - 250 \equiv 49 \pmod{65}$

Check. Since it is easy to do so, we should quickly check our answer: $49 \equiv 4 \pmod 5$, $49 \equiv 10 \pmod{13}$

Example 72. Let $p, q > 3$ be distinct primes.

(a) Show that $x^2 \equiv 9 \pmod p$ has exactly two solutions (i.e. ± 3).

(b) Show that $x^2 \equiv 9 \pmod{pq}$ has exactly four solutions (± 3 and two more solutions $\pm a$).

Solution.

(a) If $x^2 \equiv 9 \pmod p$, then $0 \equiv x^2 - 9 = (x-3)(x+3) \pmod p$. Since p is a prime it follows that $x - 3 \equiv 0 \pmod p$ or $x + 3 \equiv 0 \pmod p$. That is, $x \equiv \pm 3 \pmod p$.

(b) By the CRT, we have $x^2 \equiv 9 \pmod{pq}$ if and only if $x^2 \equiv 9 \pmod p$ and $x^2 \equiv 9 \pmod q$. Hence, $x \equiv \pm 3 \pmod p$ and $x \equiv \pm 3 \pmod q$. These combine in four different ways.
For instance, $x \equiv 3 \pmod p$ and $x \equiv 3 \pmod q$ combine to $x \equiv 3 \pmod{pq}$. However, $x \equiv 3 \pmod p$ and $x \equiv -3 \pmod q$ combine to something modulo pq which is different from 3 or -3.

Why primes >3? Why did we exclude the primes 2 and 3 in this discussion?

Comment. There is nothing special about 9. The same is true for $x^2 \equiv a^2 \pmod{pq}$ for each integer a.

Example 73. Determine all solutions to $x^2 \equiv 9 \pmod{35}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 9 \pmod{35} \\ \iff\ & x^2 \equiv 9 \pmod 5 \text{ and } x^2 \equiv 9 \pmod 7 \\ \iff\ & x \equiv \pm 3 \pmod 5 \text{ and } x \equiv \pm 3 \pmod 7 \end{aligned}$$

The two obvious solutions modulo 35 are ± 3. To get one of the two additional solutions, we solve $x \equiv 3 \pmod 5$, $x \equiv -3 \pmod 7$. [Then the other additional solution is the negative of that.]

$x \equiv 3 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 5}}_{3} - 3 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 7}}_{3} \equiv 63 - 45 \equiv 18 \pmod{35}$

Hence, the solutions are $x \equiv \pm 3 \pmod{35}$ and $x \equiv \pm 17 \pmod{35}$. [$\pm 18 \equiv \pm 17 \pmod{35}$]

Silicon slave labor. We can let Sage (more next page!) do the work for us:

```
Sage] solve_mod(x^2 == 9, 35)
```

$[(17), (32), (3), (18)]$

Sage

Any serious cryptography involves computations that need to be done by a machine. Let us see how to use the open-source computer algebra system **Sage** to do basic computations for us.

Sage is freely available at sagemath.org. Instead of installing it locally (it's huge!) we can conveniently use it in the cloud at cocalc.com from any browser.

[For basic computations, you can also simply use the textbox on our course website.]

Sage is built as a **Python** library, so any Python code is valid. For starters, we will use it as a fancy calculator.

Example 74. Let's start with some basics.

```
Sage] 17 % 12
```

5

```
Sage] (1 + 5) % 2  # don't forget the brackets
```

0

```
Sage] inverse_mod(17, 23)
```

19

```
Sage] xgcd(17, 23)
```

$(1, -4, 3)$

```
Sage] -4*17 + 3*23
```

1

```
Sage] euler_phi(84)
```

24

Example 75. Why is the following bad?

```
Sage] 3^1003 % 101
```

27

The reason is that this computes 3^{1003} first, and then reduces that huge number modulo 101:

```
Sage] 3^1003
```

$$35695912125981779196042292013307897881066394884308000526952849942124372128361032287601\\
01447396641767302556399781555972361067577371671671062036425358196474919874574608035466\\
17047063989041820507144085408031748926871104815910218235498276622866724603402112436668\\
09387969298949770468720050187071564942882735677962417251222021721836167242754312973216\\
80102291029227131545307753863985171834477895265551139587894463150442112884933077598746\\
04125161734774642865878855686737747603770909400 27$$

We know how to efficiently avoid computing huge intermediate numbers (binary exponentiation!). Sage does the same if we instead use something like:

```
Sage] power_mod(3, 1003, 101)
```

27

Example 76. (review) The solutions to $x^2 \equiv 9 \pmod{35}$ are ± 3 and $\pm 17 \pmod{35}$.

Example 77. Determine all solutions to $x^2 \equiv 4 \pmod{105}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 4 \pmod{105} \\ \iff\ & x^2 \equiv 4 \pmod 3 \text{ and } x^2 \equiv 4 \pmod 5 \text{ and } x^2 \equiv 4 \pmod 7 \\ \iff\ & x \equiv \pm 2 \pmod 3 \text{ and } x \equiv \pm 2 \pmod 5 \text{ and } x \equiv \pm 2 \pmod 7 \end{aligned}$$

At this point, we see that there are $2^3 = 8$ solutions.

For instance, let us find the solution corresponding to $x \equiv 2 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv -2 \pmod 7$:

$$x \equiv 2 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)^{-1}_{\bmod 3}]}_{-1} + 2 \cdot 3 \cdot 7 \cdot \underbrace{[(3 \cdot 7)^{-1}_{\bmod 5}]}_{1} - 2 \cdot 3 \cdot 5 \cdot \underbrace{[(3 \cdot 5)^{-1}_{\bmod 7}]}_{1} \equiv -70 + 42 - 30 = -58 \equiv 47$$

Similarly, we find all eight solutions (note how the solutions pair up):

$\pmod 3$	$\pmod 5$	$\pmod 7$	$\pmod{105}$
2	2	2	2
−2	−2	−2	−2
2	2	−2	47
−2	−2	2	−47
2	−2	2	23
−2	2	−2	−23
−2	2	2	37
2	−2	−2	−37

The complete list of solutions is: $\pm 2, \pm 23, \pm 37, \pm 47$

Silicon slave labor. Once we are comfortable doing it by hand, we can easily let Sage do the work for us:

```
Sage] crt([2,2,-2], [3,5,7])
```

47

```
Sage] solve_mod(x^2 == 4, 105)
```

$[(37), (82), (58), (103), (2), (47), (23), (68)]$

Review: quadratic residues

Definition 78. An integer a is a **quadratic residue** modulo n if $a \equiv x^2 \pmod n$ for some x.

Important note. Products of quadratic residues are quadratic residues.

Example 79. List all quadratic residues modulo 11.

Solution. We compute all squares: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 5$, $(\pm 5)^2 \equiv 3$. Hence, the quadratic residues modulo 11 are $0, 1, 3, 4, 5, 9$.

Important comment. Exactly half of the 10 nonzero residues are quadratic. Can you explain why?

[*Hint.* $x^2 \equiv y^2 \pmod p \iff (x-y)(x+y) \equiv 0 \pmod p \iff x \equiv y$ or $x \equiv -y \pmod p$]

Example 80. List all quadratic residues modulo 15.

Solution. We compute all squares modulo 15: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 1$, $(\pm 5)^2 \equiv 10$, $(\pm 6)^2 \equiv 6$, $(\pm 7)^2 \equiv 4$. Hence, the quadratic residues modulo 15 are $0, 1, 4, 6, 9, 10$.

Important comment. Among the $\phi(15) = 8$ invertible residues, the quadratic ones are $1, 4$ (exactly a quarter). Note that 15 is of the form $n = pq$ with p, q distinct primes.

Armin Straub
straub@southalabama.edu

Theorem 81. Let p, q, r be distinct odd primes.

- The number of invertible residues modulo n is $\phi(n)$.
- The number of invertible quadratic residues modulo p is $\frac{\phi(p)}{2} = \frac{p-1}{2}$.
- The number of invertible quadratic residues modulo pq is $\frac{\phi(pq)}{4} = \frac{p-1}{2}\frac{q-1}{2}$.
- The number of invertible quadratic residues modulo pqr is $\frac{\phi(pqr)}{8} = \frac{p-1}{2}\frac{q-1}{2}\frac{r-1}{2}$.
- ...

Proof.

- We already knew that the number of invertible residues modulo n is $\phi(n)$.
- Think about squaring all residues modulo p to make a complete list of all quadratic residues. Let a^2 be one of the nonzero quadratic residues. As we observed earlier, $x^2 \equiv a^2 \pmod{p}$ has exactly 2 solutions, meaning that exactly two residues (namely $\pm a$) square to a^2. Hence, the number of invertible quadratic residues modulo p is half the number of invertible residues modulo p.
- Again, think about squaring all residues modulo pq to make a complete list of all quadratic residues. Let a^2 be one of the invertible quadratic residues. By the CRT, $x^2 \equiv a^2 \pmod{pq}$ has exactly 4 solutions (why is it important that a is invertible here?!), meaning that exactly four residues square to a^2. Hence, the number of invertible quadratic residues modulo pq is a quarter of the number of invertible residues modulo pq.
- Spell out the situation modulo pqr! □

Comment. Make similar statements when one of the primes is equal to 2.

Example 82. (bonus!) What is the total number of quadratic residues modulo pqr if p, q, r are distinct odd primes? (To collect a bonus point, send me the answer and a short explanation by next week.)

The Blum-Blum-Shub PRG

(Blum-Blum-Shub PRG) Let $M = pq$ where p, q are large primes $\equiv 3 \pmod{4}$.
From the seed y_0, we generate $y_{n+1} \equiv y_n^2 \pmod{M}$.
The random bits x_n we produce are $y_n \pmod{2}$ (i.e. $x_n = \text{least bit of}(y_n)$).

Comments next class.

Example 83. Generate random bits using the B-B-S PRG with $M = 77$ and seed 3.

Solution. With $y_0 = 3$, we have $y_1 \equiv y_0^2 = 9$, followed by $y_2 \equiv y_1^2 \equiv 4 \pmod{77}$, $y_3 \equiv 16$, $y_4 \equiv 25$, $y_5 \equiv 9$, so that the values y_n now start repeating.

These numbers are, however, not the output of the PRG. We only output the least bit of the numbers y_n, i.e. the value of $y_n \pmod{2}$. For $y_1 \equiv 9$ we output 1, for $y_2 \equiv 4$ we output 0, for $y_3 \equiv 16$ we output 0, for $y_4 \equiv 25$ we output 1, and so on.

In other words, the seed 3 produces the sequence $1, 0, 0, 1, 1, 0, 0, 1, 1, 0, \ldots$ of period 4.

Comment. Note that it was completely to be expected that the numbers repeat. In fact, we immediately see that the number of possible y_n is at most the number of invertible quadratic residues, of which there are only $\phi(77)/4 = 15$.