Introduction to Cryptography

TEK 4500 (Fall 2021)
Problem Set 7

Problem 1. (*Optional*):
Read more about the Dual EC DBRG story.

- *Where did I leave my keys? Lessons from the Juniper Dual EC incident* [CMG+18]. Short version of the full academic paper [CCG+16].
- Various blog posts by Matthew Green:
  - *On the Juniper backdoor* (link).
  - *The strange story of "Extended Random"* (link).
  - *The Many Flaws of Dual_EC_DRBG* (link).
  - *Hopefully the last post I'll ever write on Dual EC DRBG* (link).
  - *Looking back at the Snowden revelations* (link).
  - *RSA warns developers not to use RSA products* (link).
  - *A few more notes on NSA random number generators* (link).
- *Dual EC: A Standardized Back Door* [BCKL15], summary article with a good timeline of the different events.
- Who replaced the Q value in Juniper's ScreenOS? A very recent Bloomberg article provides more details: *Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role* (link).
- *Dual EC DRBG*, good summary site with plenty of links for further reading (link).

Problem 2. How random are you?
Are you a good source of randomness? Try to "beat" the oracle at `https://people.ischool.berkeley.edu/~nick/aaronson-oracle/`, which attempts to predict your next key press. Problem passed if you manage to get it down to 50% (be honest!).

$\underline{\mathbf{Exp}^{\mathsf{prg}}_{G}(\mathcal{A})}$

1: $b \leftarrow \{0,1\}$
2: $s \xleftarrow{\$} \{0,1\}^{\ell}$
3: $U_1 \leftarrow G(s)$
4: $U_0 \xleftarrow{\$} \{0,1\}^{L}$
5: $b' \leftarrow A(U_b)$
6: **return** $b' \stackrel{?}{=} b$

$$\mathbf{Adv}^{\mathsf{prg}}_{G}(\mathcal{A}) = |2 \cdot \Pr[\mathbf{Exp}^{\mathsf{prg}}_{G}(\mathcal{A}) \Rightarrow \mathsf{true}] - 1| = |\Pr[\mathcal{A}(U_1) \Rightarrow 1] - \Pr[\mathcal{A}(U_0) \Rightarrow 1]|$$

Figure 1: PRG security experiment and PRG-advantage definition for a function $G\colon \{0,1\}^{\ell} \to \{0,1\}^{L}$.

Problem 3.

The *linear congruential generator* is a very simple PRNG defined as follows for a *public* modulus m and *private* constants a, b:

$$s_i \leftarrow (a \cdot s_{i-1} + b) \pmod{m} \tag{1}$$

Here $0 \leq s_0 \leq m-1$ is the initial (secret) seed, and all the s_i's are the output of the generator for $i > 0$.

Explain how you can completely break the linear congruential generator, assuming you've observed $s_1, s_2, \ldots$

Note: In class we only defined PRNG's as operating on bits (and returning bits), but it's perfectly fine to define them on other domains and ranges too. In this case you should compare the output of the generator with a sequence of truly random numbers $0 \leq x_i \leq m-1$.

Problem 4.

Let G be a secure PRNG. In all of the following cases, determine whether G' is also a secure PRNG.

a) $G'(s) = G(\overline{s})$, where $\overline{s}$ is the bitwise complement of s (i.e., all of the bits in s flipped).

b) $G'(s) = \overline{G(s)}$

c) $G'(s) = G(0^{|s|} \| s)$

d) $G'(s) = G(s) \| G(s+1)$

e) $G'(s) = G(s) \| s$

f) $G'(s) = G(s) \| G(\overline{s})$

Problem 5. [Problem 3.21 in [BS]]

In this exercise we'll see that a secure PRNG can fail to be secure if the seed is not uniformly distributed. Let $G\colon \{0,1\}^\ell \to \{0,1\}^L$ be a secure PRNG.

a) Define a new PRNG $G'\colon \{0,1\}^{\ell+1} \to \{0,1\}^{L+1}$ as follows:

$$G'(s\|t) = G(s)\|t,$$

where $s \in \{0,1\}^\ell$ and $t \in \{0,1\}$. Show that G' is a secure PRNG.

b) Suppose the seed for G' chosen so that the last bit t is always 0. Show that this makes G' insecure. What's the advantage of your attack?

c) Construct a secure PRNG $G''\colon \{0,1\}^{\ell+1} \to \{0,1\}^{L+1}$ that becomes insecure if its seed is chosen so that the *parity* of the bits in the seed is always 0.

References

[BCKL15] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted hessian curves. *IACR Cryptol. ePrint Arch.*, page 781, 2015. https://eprint.iacr.org/2015/781.

[BS] Dan Boneh and Victor Shoup. *A Graduate Course in Applied Cryptography*, (version 0.5, Jan. 2020). https://toc.cryptobook.us/.

[CCG+16] Stephen Checkoway, Shaanan Cohney, Christina Garman, Matthew Green, Nadia Heninger, Jacob Maskiewicz, Eric Rescorla, Hovav Shacham, and Ralf-Philipp Weinmann. A systematic analysis of the juniper dual EC incident. *IACR Cryptol. ePrint Arch.*, page 376, 2016. https://eprint.iacr.org/2016/376.

[CMG+18] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. Where did I leave my keys?: lessons from the juniper dual EC incident. *Commun. ACM*, 61(11):148–155, 2018. https://doi.org/10.1145/3266291.