Tutorial 3

Gidon Rosalki

2025-11-19

Notice: If you find any mistakes, please open an issue at `https://github.com/robomarvin1501/notes_intro_to_crypto`

1 Reminder

We began with One Time Pads (OTPs), that enable *perfect secrecy*, but have the problems of single use keys, and exceedingly long keys. We then moved on to *Indistinguishable Encryptions*, and *PRG*s, which enabled smaller keys. We then continued on to create a scheme, using *Pseudo Random Functions* that was resistant to *Chosen Plaintext Attacks*, and showed that PRGs are equivalent to PRFs.

Exercise 1. *Given* $\Pi_1 = (KeyGen_1, Enc_1, Dec_1)$*, and* $\Pi_2 = (KeyGen_2, Enc_2, Dec_2)$*, one of* Π_1, Π_2 *is IND. Create a scheme* Π *that is IND.*

Solution. Π will be as follows:

- $KeyGen\left(1^n\right)$: The key will be constructed of 2 parts: (k_1, k_2), where for $i \in \{1, 2\}$ k_i comes from $KeyGen_i$
- $Enc\left(k, m\right)$: $Enc_{k_2}\left(Enc_{k_1}\left(m\right)\right)$
- $Dec\left(k, c\right)$: $Dec_{k_1}\left(Dec_{k_2}\left(c\right)\right)$

The correctness of the scheme is obvious from the construction, since both the base schemes are correct. We must now prove that it is IND-secure:

Let us assume towards contradiction that the scheme is not IND-secure, so there exists an polynomial adversary A that can win the IND game against Π. There are 2 cases:

Case 1: Π_1 is IND-secure, and Π_2 is not. We will thus build the adversary B that breaks Π_1 as follows:

1. It does this by generating m_0, m_1 from A
2. $k_2 \leftarrow KeyGen_2\left(1^n\right)$
3. Get $c = Enc_{k_1}\left(m_b\right)$
4. Compute $Enc_{k_2}\left(c\right)$, and send it to A
5. A returns b', which B then returns

Case 2: Π_2 is IND-secure, and Π_1 is not. We will build B that breaks Π_2 as follows:

1. Generate m_0, m_1 from A
2. $k_1 \leftarrow KeyGen_1$
3. Create p_0, p_1 via $Enc_{k_1}\left(m_i\right)$
4. Send these for encryption by Enc_{k_2}, and then send those to A, which can by assumption differentiate them.

In both cases, we have built an adversary that can break the IND-secure scheme, which is a contradiction, and so we can conclude that Π is IND-secure. ☐

Exercise 2. *Let there be a PRF* $F_k, G_k : \{0,1\}^n \to \{0,1\}^n$*, which means that*

$$\forall PPT\ D : \Pr_{k \leftarrow \{0,1\}^n}\left[D^{F_k(\cdot)} = 1\right] - \Pr_{r \leftarrow Funcs_{n \to n}}\left[D^{r(\cdot)} = 1\right] < neg\left(n\right)$$

In short, we cannot distinguish between the output of a PRF, and a truly random function.
Prove / Disprove

$$\forall PPT\ D : \left|\Pr\left[D^{F_k(\cdot)} = 1\right] - \Pr\left[D^{G_k(\cdot)} = 1\right]\right| \leq neg\left(n\right)$$

Or in Spanish, para cada PPT D, no podemos distinguir entre la salida de dos PRF.
Finally, in English, sbe rirel CCG Q, jr pnaabg qvfgvathvfu orgjrra gur bhgchg bs gjb CESf.

Solution. We shall prove this as follows:

$$\begin{aligned}\forall D:\ \left|\Pr\left[D^{F_k}=1\right]-\Pr\left[D^{G_k}=1\right]\right| &\le \left|\Pr\left[D^{F_k}=1\right]-\Pr_{r\leftarrow Funcs}\left[D^{r}=1\right]\right|+\left|\Pr\left[D^{G_k}=1\right]-\Pr_{r\leftarrow Funcs}\left[D^{r}=1\right]\right|\\ &\le neg+neg\\ &= neg\end{aligned}$$

As required (since adding together 2 negligible functions is still negligible). □

Exercise 3. *Given two functions $F_k, G_k : \{0,1\}^n \to \{0,1\}^n$, where one of them is a PRF, prove or disprove that H_{k_1,k_2} is a PRF, where*

$$H_{k_1,k_2}(x) = G_{k_1}\left(F_{k_2}(x)\right)$$

Solution. This is not the case. There are 2 cases:

Case 1: G is a PRF, and F is not. We may then set $F(x) = 0$. As a result

$$H_{k_1,k_2} = G_{k_1}(0)$$

Which is a constant output, and as a result, H_{k_1,k_2} is definitely not a PRF.

Case 2: Here F is a PRF, and G is not. Let us set $G(x) = 0$:

$$H_{k_1,k_2} = G_{k_1}\left(F_{k_2}(x)\right) = 0$$

Which is trivially not pseudorandom. □

Exercise 4. *Let there be a PRF F. We will create*

$$H_k(x) = F_{F_k(0)}(x)\,\|F_k(x)$$

Prove or disprove that H is a PRF.

Solution. H is *not* a PRF. Let there be an oracle $z \leftarrow \{H, r\}$, and we will construct the distinguisher $D^{z(\cdot)}$ as follows:

1. $z(0) = L$
2. Compute $F_L(8)$
3. $z(8)$

If $z = H_k$ then $z(8) = F_{F_k(0)}(8)\,\|F_k(8)$. Note that $F_{F_k(0)}(8) = F_L(8)$. Therefore, we can distinguish between this, and the output of a random function, where this would simply be random noise. □

Exercise 5. *Given*

$$W_{k_1,k_2}(x) = F_{F_{k_1}(0)}\|F_{k_2}(x)$$

Where F is a PRF. Is W a PRF?

Solution. Let us begin by proving the following 2 theorems:

Theorem 1. *$H_k(x) = F_{F_k(0)}$ is a PRF*

Proof . We will begin with the distinguisher

$$\begin{aligned}\left|\Pr\left[D^{F_{F_k(0)}(\cdot)}=1\right]-\Pr\left[D^{r(\cdot)}=1\right]\right| &\le \left|\Pr\left[D^{F_{F_k(0)}(\cdot)}\right]-\Pr\left[D^{F_{r(0)}(\cdot)}=1\right]\right|-\left|\Pr\left[D^{F_{r(0)}(\cdot)}=1\right]-\Pr\left[D^{r(\cdot)}=1\right]\right|\\ &\le neg\end{aligned}$$

□

Theorem 2. *$G_{k_1,k_2}(x) = L_{k_1}(x)\,\|F_{k_2}(x)$ is a PRF, where L, F are PRFs.*

Proof . We want to show that $L_{k_1}(x)\,\|F_{k_2}(x)$ is a PRF, or indistinguishable from concatenating two parts of random noise $r(\cdot)\,\|r(\cdot)$. We may do this with a hybrid proof, by showing that $L_{k_1}\|r(\cdot)$ is indistinguishable from the PRF, and then that it is also indistinguishable from $r(\cdot)\,\|r(\cdot)$. □

□