Observe that a block cipher can be used to construct a PRG:

$F: \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher

Define $G: \{0,1\}^\lambda \to \{0,1\}^{\ell n}$ as

$$G(k) = F(k,1) \| F(k,2) \| \cdots \| F(k,\ell)$$

← this stream cipher allows random access!

↑ string concatenation

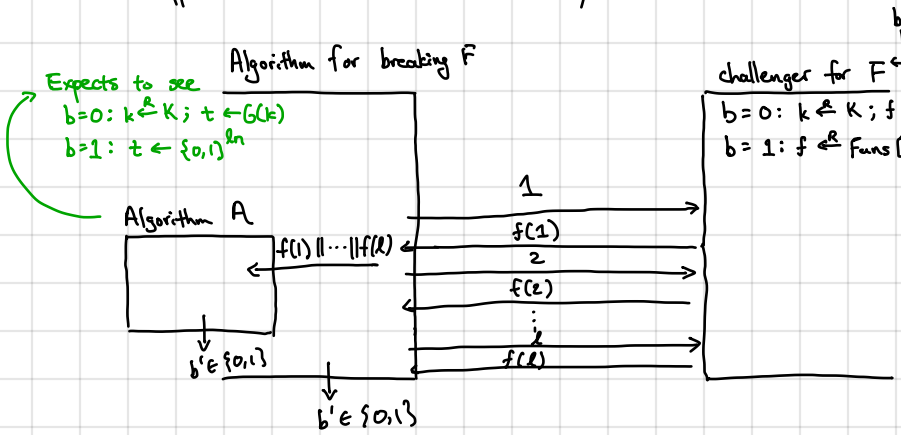
↑ write input as an n-bit string (just require that $n > \log \ell$)

we said PRP above (will revisit this) ↘

Theorem. If F is a secure PRF, then G is a secure PRG.

Proof. As usual, we show the contrapositive: if G is not a secure PRG, then F is not a secure PRF.

Suppose we have efficient adversary A for G. We use A to build adversary for F:



1. If ℓ = poly, then B is efficient
2. If $b=0$: B sends $G(k)$ to A where k is a uniformly random key

   If $b=1$: B sends uniformly random string (f is random function) to A
3. $\text{PRFAdv}[B,F] = |\Pr[b'=1 \mid b=0] - \Pr[b'=1 \mid b=1]|$

$= |\Pr[A \text{ outputs } 1 \mid b=0] - \Pr[A \text{ outputs } 1 \mid b=1]|$

$= \text{PRGAdv}[A,G]$

which is non-negligible by assumption.

But... we used a block cipher (PRP) in our construction above. Does the proof still go through?

Not quite...

for a random function, $f(1) = f(2)$ with probability $\frac{1}{2^n}$

for a random permutation, $f(1) = f(2)$ with probability 0

} but 2^{-n} might be very very small... adversary won't notice unless it sees a "collision" [i.e., two values x,y where $f(x) = f(y)$]

PRF Switching Lemma. Let $F: K \times X \to X$ be a secure PRP. Then, for any Q-query adversary A:

$$|\text{PRPAdv}[A,F] - \text{PRFAdv}[A,F]| \leq \frac{Q^2}{2|X|}$$

Proof Idea. Adversary essentially cannot tell the difference unless it sees a collision. If there is no collision, then it is just seeing random values. How many queries before there is a collision? Birthday paradox: $Q \sim \sqrt{|X|}$

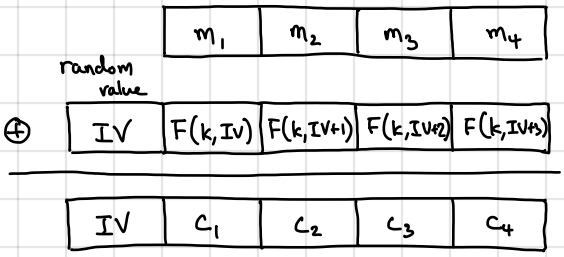
Take-away: If $|X|$ is large (e.g., exponential), then we can use a PRP as a PRF.

- 3DES: $n = 64$ so $|X| = 2^{64}$ [if adversary makes $\ll 2^{32}$ queries, then can use it as a PRF]
- AES: $n = 128$ so $|X| = 2^{128}$ [if adversary makes $\ll 2^{64}$ queries, then can use it as a PRF]

Thus far: PRP/PRF in "counter mode" gives us a stream cipher (one-time encryption scheme)

How do we reuse it? Choose a random starting point (called an initialization vector) ← typically, the IV is divided into a nonce (value that does not repeat) and a counter: IV = nonce || counter

"randomized counter mode"



divide message into blocks (based on block size of PRF)

ciphertext

observe: ciphertext is longer than the message (required for CPA security)

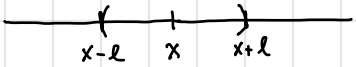
Theorem: Let $F: K \times X \to Y$ be a secure PRF and let Π_{CTR} denote the randomized counter mode encryption scheme from above for ℓ-block messages ($M = X^{\leq \ell}$). Then, for all efficient CPA adversaries A, there exists an efficient PRF adversary B such that

$$CPAAdv[A, \Pi_{CTR}] \leq \frac{4Q^2\ell}{|X|} + 2 \cdot PRFAdv[B, F]$$

↖ Q: number of encryption queries
ℓ: number of blocks in message

Intuition:

1. If there are no collisions (i.e., PRF never evaluated on the same block), then it is as if everything is encrypted under a fresh one-time pad.
2. Collision event: $(x, x+1, \ldots, x+\ell-1)$ overlaps with $(x', x'+1, \ldots, x'+\ell-1)$ when $x, x' \xleftarrow{R} X$



↖ probability that x' lies in this interval is $\leq \frac{2\ell}{|X|}$

There are $\leq Q^2$ possible pairs (x, x'), so by a union bound,

$$Pr[\text{collision}] \leq \frac{2\ell Q^2}{|X|}$$

3. Remaining factor of 2 in advantage due to intermediate distribution (hybrid argument):

Encrypt m_0 with PRF ↘ $PRFAdv[B,F] + \frac{2\ell Q^2}{|X|}$
Encrypt m_0 with fresh one-time pad ↘ 0
Encrypt m_1 with fresh one-time pad ↘ $PRFAdv[B,F] + \frac{2\ell Q^2}{|X|}$
Encrypt m_1 with PRF

Interpretation: If $|X| = 2^{128}$ (e.g., AES), and messages are 1 MB long (2^{16} blocks) and we want the distinguishing advantage to be below 2^{-32}, then we can use the same key to encrypt

$$Q \leq \sqrt{\frac{|X| \cdot 2^{-32}}{4\ell}} = \sqrt{\frac{2^{96}}{2^{18}}} = \sqrt{2^{78}} = 2^{39} \quad (\sim 1 \text{ trillion messages!})$$