BLOCK CIPHERS

As we know, PRFs are enough to do all the crypto in MINICRYPT: SKE and MACs.

But we saw sometimes we need PRPs: given K we can invert $F(K, x)$ efficiently. In practice, PRPs are called BLOCK CIPHERS: DES and AES.

Remark: Neither of them is PROVABLY

secure based on standard assumptions.
However, their design is inspired by standard results in provable security.
For DES: Feistel Network. A way to turn a PRF into a PRP. Let $F: \{0,1\}^n \to \{0,1\}$ be a function. Consider the following permutation over $\{0,1\}^{2n}$:

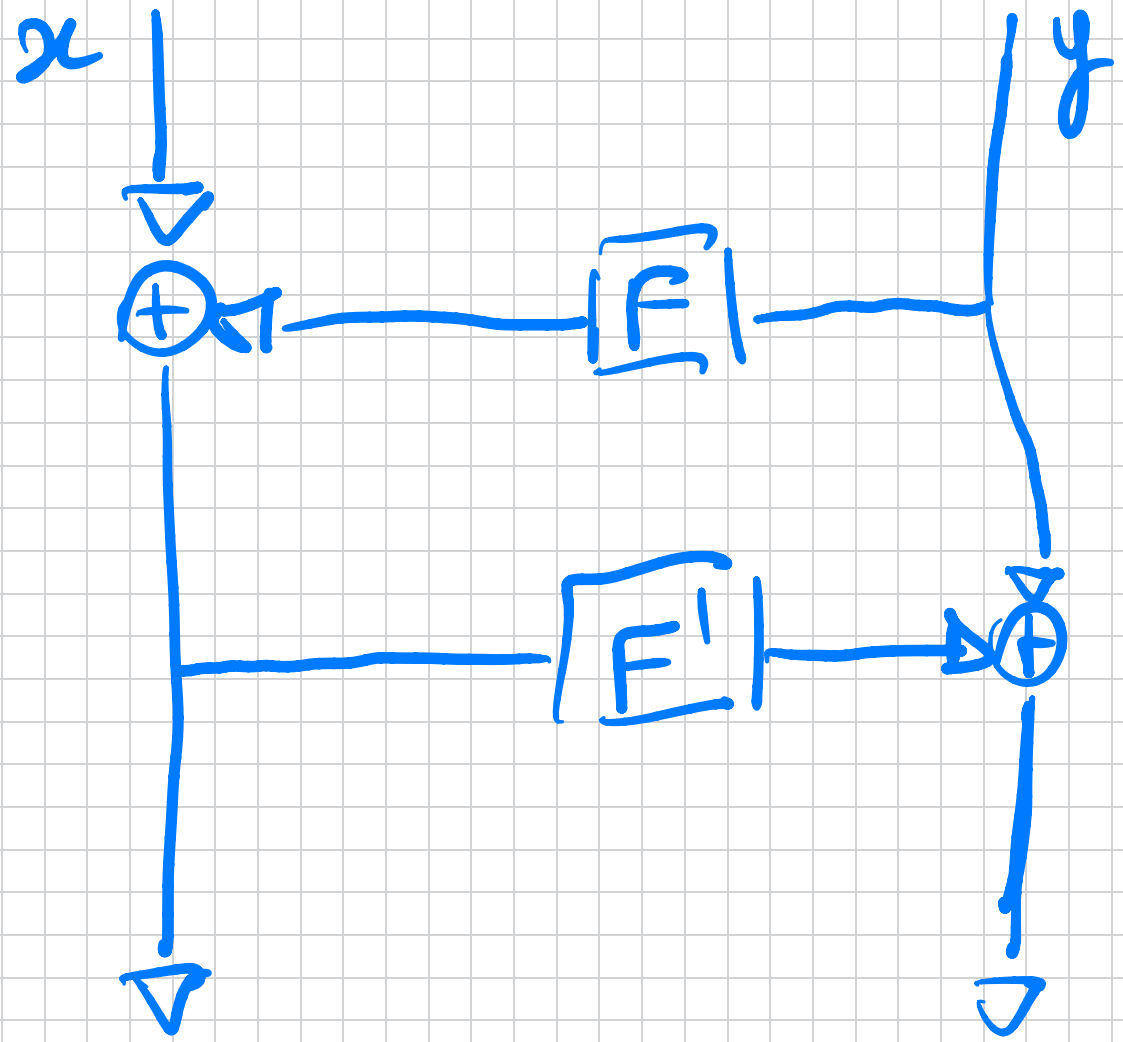
$$\psi_F(x,y) = (y, x \oplus F(y))$$

$$= (x', y') \in \{0,1\}^{2n}$$

$$\psi_F^{-1}(x', y') = (F(x') \oplus y', x')$$

Is it pseudorandom? No because the first 1/2 of our outputs is some of second 1/2 of input!

Idea: Do it several times.



$x \oplus F(y)$ $\qquad$ $y \oplus F'(x \oplus F(y))$

$$\Psi_{FF'}(x,y) = \Psi_{F'}(\Psi_F(x,y))$$

In reality F, F' are sets of $F(K_1, \cdot)$ and $F(K_2, \cdot)$ for independent keys K_1, K_2.

Are 2 rounds enough? No, but almost.

Note: $\Psi_{F,F'}(x, y) \oplus \Psi_{F,F'}(x', y)$

$= (x \oplus x', \longrightarrow)$

$\Rightarrow$ This implies a distinguisher against PSEUDORANDOMNESS.

THM 3 rounds of Feistel with a PRF (Wide pendent keys) are a PRP.

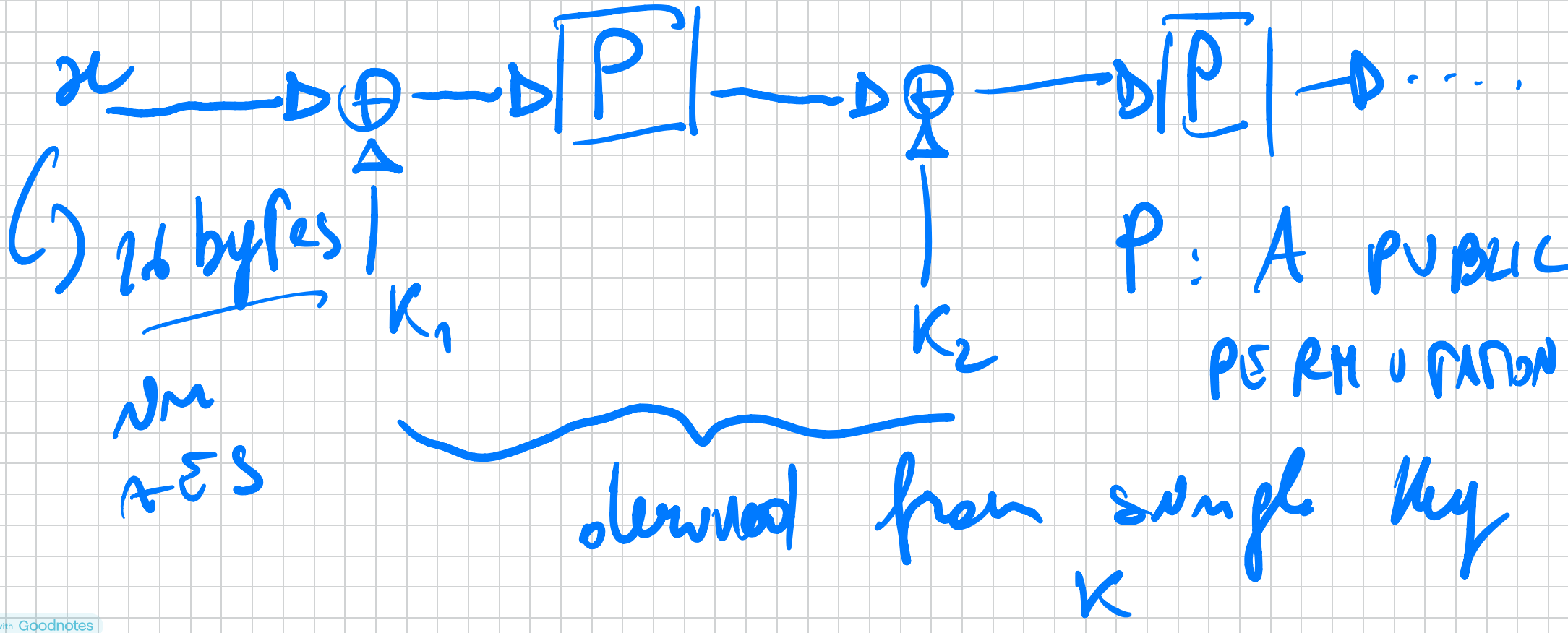
Intuition: Two rounds are enough if y's are DISTINCT. The first round makes the y's DISTINCT except with small prob.

DES: Uses this construction with HEURISTIC F, for 18 rounds

and pseudorandom keys $K_1, \ldots, K_{18}$ derived all from some key K.

Main problem with DES: key is kind of short. Easy fix: Double encryption does not work (some brute force complexity because of meet-in-the-middle attacks). Solution: 3DES. Not very efficient; for this reason a new standard was made: AES.

The provable security of AES is even worse: we know very little. This is an instantiation of SUBSTITUTION PERMUTATION NETWORKS (SPNs).



LEMMA For every UNBOUNDED attacker making $q \in poly(\lambda)$ queries the following are INDISTINGUISHABLE:

- S: $\psi_{F,F'}(\cdot,\cdot)$ for $F,F' \leftarrow R(\lambda, m, n)$

- R: $R \leftarrow R(\lambda, 2m, 2n)$

So long as the queries $(x_1, y_1), \ldots, (x_q, y_q)$

are "UNIQUE" ($y_i \neq y_j$ for $i \neq j$).

Proof (of THM). We consider some keybreaks:

- $T : (x, y) \mapsto \psi_{F_{k_3}}(\psi_{F_{k_2}}(\psi_{F_{k_1}}(x, y)))$

  $k_1, k_2, k_3 \leftarrow K$.

- $S : (x, y) \mapsto \psi_{F, F'}(\psi_{F''}(x, y))$

  $F, F', F'' \leftarrow R(\lambda, m, n)$

-) R : (x, y) $R \leftarrow R(\lambda, 2n, 2n)$

$\mapsto R(x, y)$ ↳ RANDOM FUNCTION.

-) P : (x, y) $P \leftarrow P(\lambda, 2n, 2n)$

$\mapsto P(x, y)$ ↳ RANDOM PERMUTATION

$T(\lambda) \overset{\sim}{\approx}_c S(\lambda)$. Simple reduction To PRF security.

$R(\lambda) \not\simeq_c P(\lambda)$:

$$\Pr\left[\exists N, i, j \text{ s.t. } (x_i, y_i) : R(x_N, y_N) = R(x_j, y_j)\right]$$

$$\leq \binom{q}{2} 2^{-2n} = \text{negl}(n).$$

$S(\lambda) \approx R(\lambda)$. Here, we use the lemma. How? We prove that for every $(x_1, y_1), \ldots, (x_q, y_q)$ the prob. that the outputs $\psi_{F(1)}(x_i, y_i)$ are NOT unique is negligible. Then we can invoke the lemma.

Let (x_j, y_j), (x_i, y_i) be the inputs. s.t. $(x_j, y_j) \neq (x_i, y_i)$. Assume first that $y_j = y_i$ so

$x_n \neq x_i$. Then:

$$y_n'' = x_n \oplus F''(y_n)$$

$$\neq x_i \oplus F''(y_i)$$

$$= x_i \oplus F''(y_i) = y_i''$$

Now assume $y_n \neq y_i$. Then:

$$x_i \oplus x_i = F''(y_n) \oplus F''(y_i)$$

$$\Rightarrow \text{Pr}[F''(y_n) \oplus F''(y_i) = x_n - x_i]$$

$$\leq 2^{-n}$$

$$\Rightarrow \Pr[C \text{ not unique}] \leq \binom{q}{2} \cdot 2^{-n}$$

$$= \mathrm{negl}(n).$$

$$\Rightarrow T(\lambda) \overset{c}{\approx} S(\lambda) \overset{c}{\approx} R(\lambda)$$

$$\overset{c}{\approx} P(\lambda) \qquad \blacksquare$$