CS171: Cryptography

Lecture 8

Sanjam Garg

All Photos are by Unknown Author and are licensed under CC BY-SA

Block Ciphers

Block Ciphers: Recall

- Keyed Permutation
$$F: \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$$
- n is the key length and ℓ is the block length

- Security: F should be indistinguishable from a uniform permutation over $\{0,1\}^\ell$.
  - Typically, want strong security.
- Interested in concrete security. For key of length n, security is desired against attacker running in time 2^n.

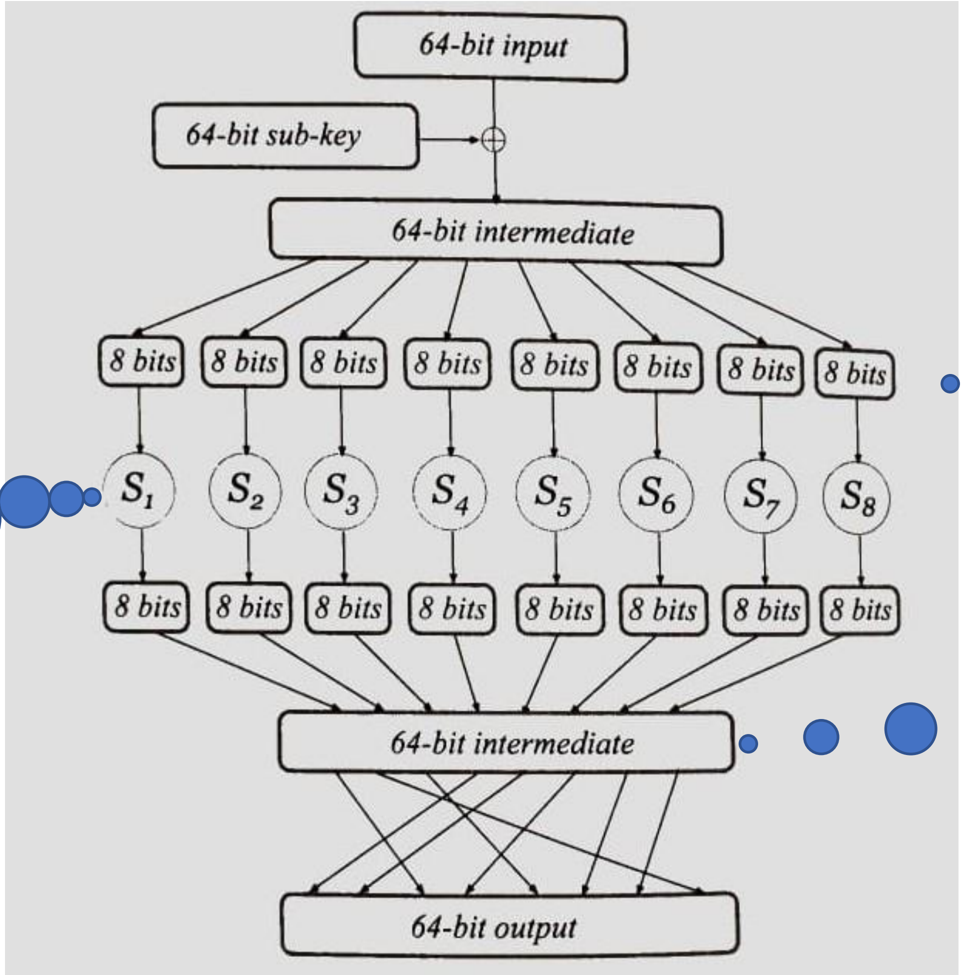
Challenge involved

- F should be indistinguishable from a uniform permutation over $\{0,1\}^{\ell}$.
- If inputs x and x' differ in one bit then what relation between $F_k(x)$ and $F_k(x')$ can we expect?
  - How many bits do we expect to change?
  - Which bits do we expect to change?

Design Paradigms

- Substitution-permutation networks (SPNs)
- Feistel networks

Add Mixing Permutation



Invertible!

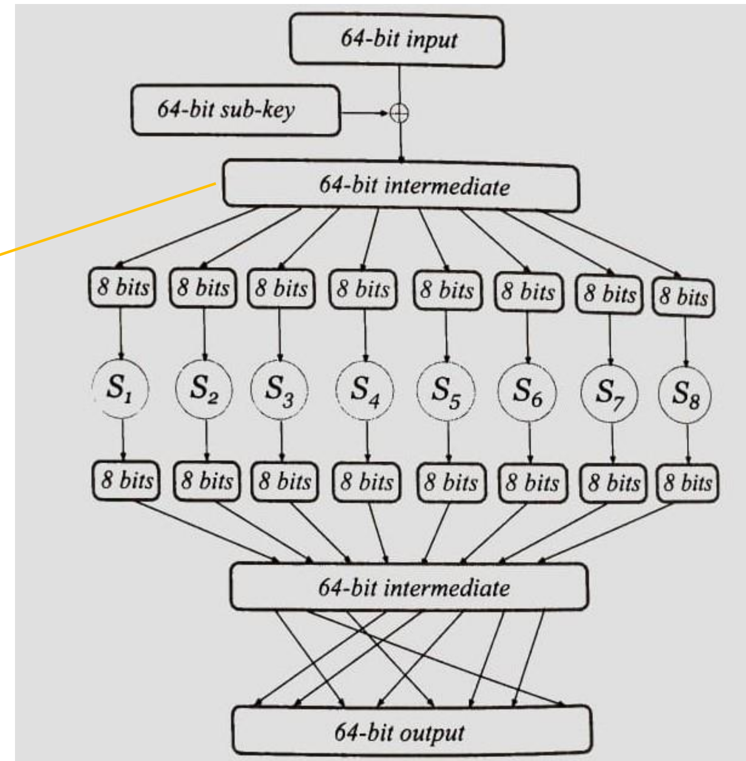
Replace Random permutations with S-boxes!

Public Mixing Permutation!

Attacking 1-Round SPN (no output key mixing)

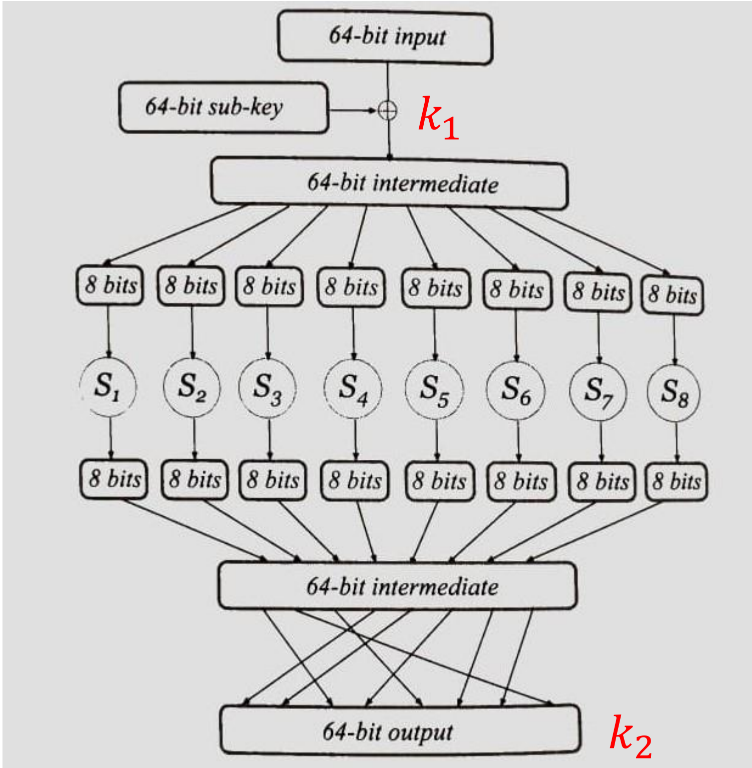
- One Round SPN

Compute z



- Find k given x, y, where $y = F_k(x)$?
- $k = x \oplus z$

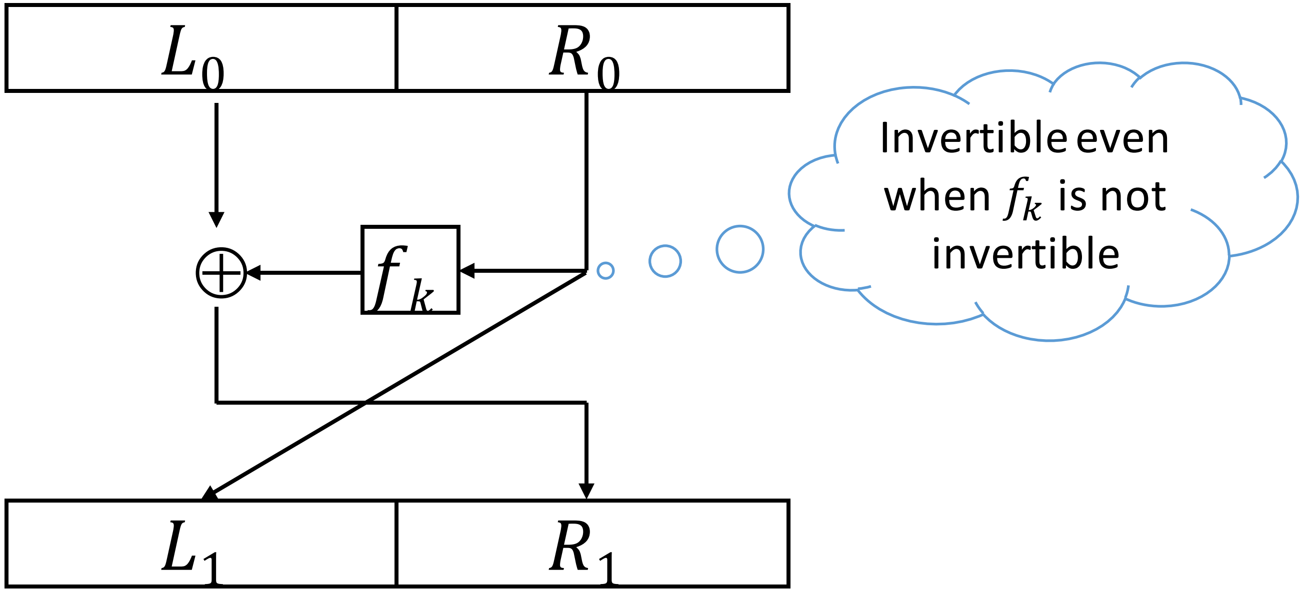
Attacking 1-Round SPN (with output key mixing)



- Find $k = (k_1, k_2)$
- $\forall k_1$ there is a unique k_2.
- Running time?
  - $\approx 2^{64}$
- Can we have a better attack?
- Same attack: S-box by S-box!
- Running time?
  - $\approx 8 \cdot 2^8$

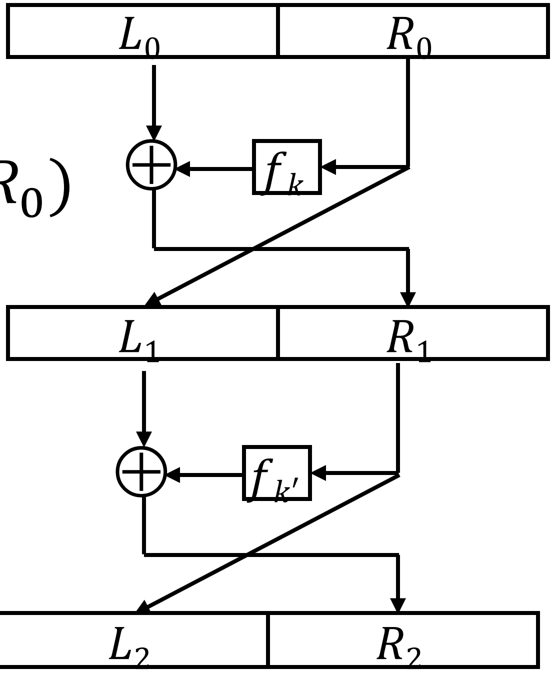
Feistel Networks

- In SPNs, the starting components were *invertible*.
- In Feistel Networks, we build invertible permutations starting from non-invertible components



Security:

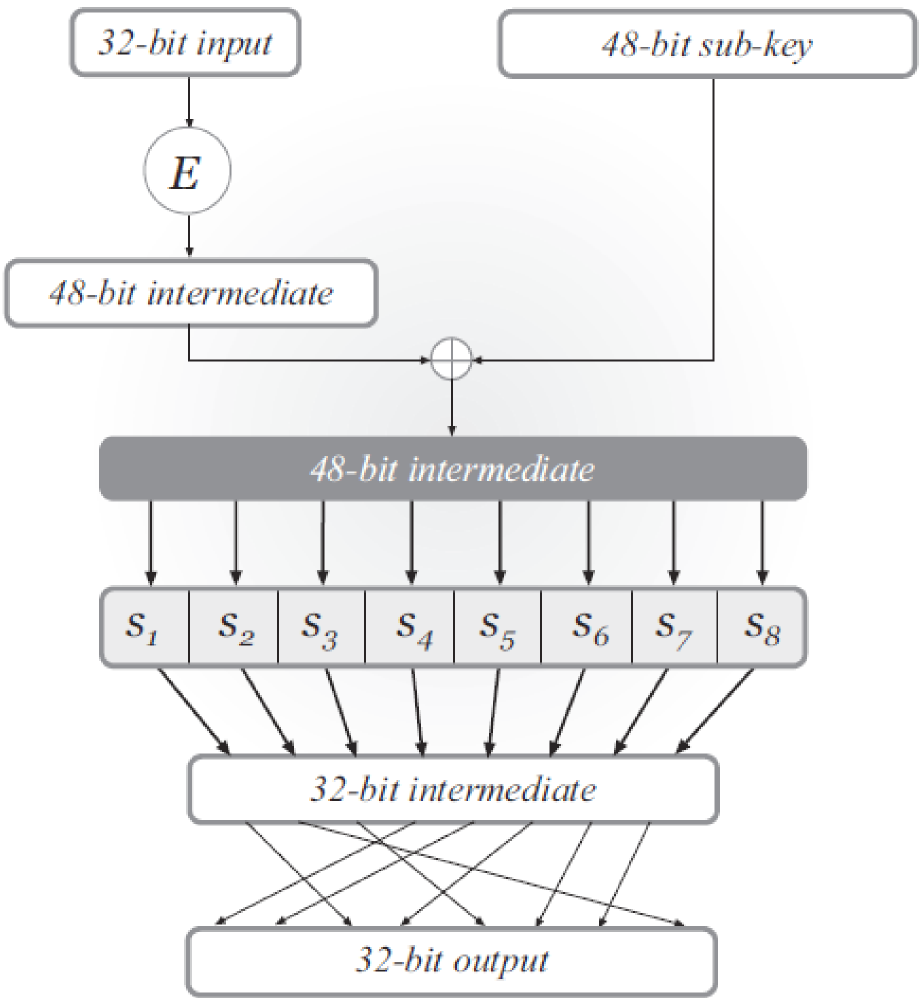
- Is 1 round secure?
  - No! Observe correlations between computations on (L_0, R_0) and $(L_0{}', R_0)$
- Is 2 round secure?
  - No! Compute on (L_0, R_0) and (L'_0, R_0)
  - L_0 and L'_0 differ in one bit
- Need 3 or more rounds



The Data Encryption Standard

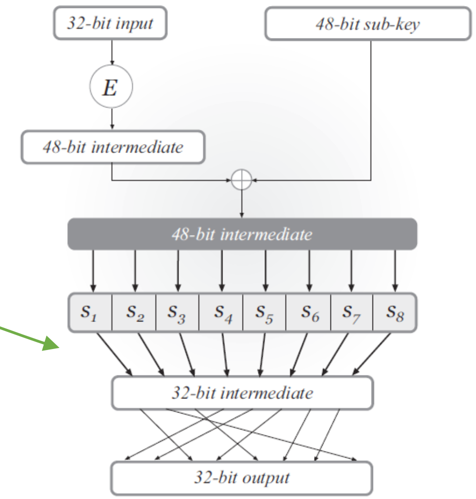
- Developed in 1970 and adopted in 1977
- 56-bit keys and 64-bit block length
- Attacks in $\approx 2^{56}$ time (too small), security can be upgrade by using triple DES
- 16-round Feistel network
    - Uses the same mangler function in each rounds
    - The mangler function is basically an SPN
    - Different sub-keys for each round are derived from the master key

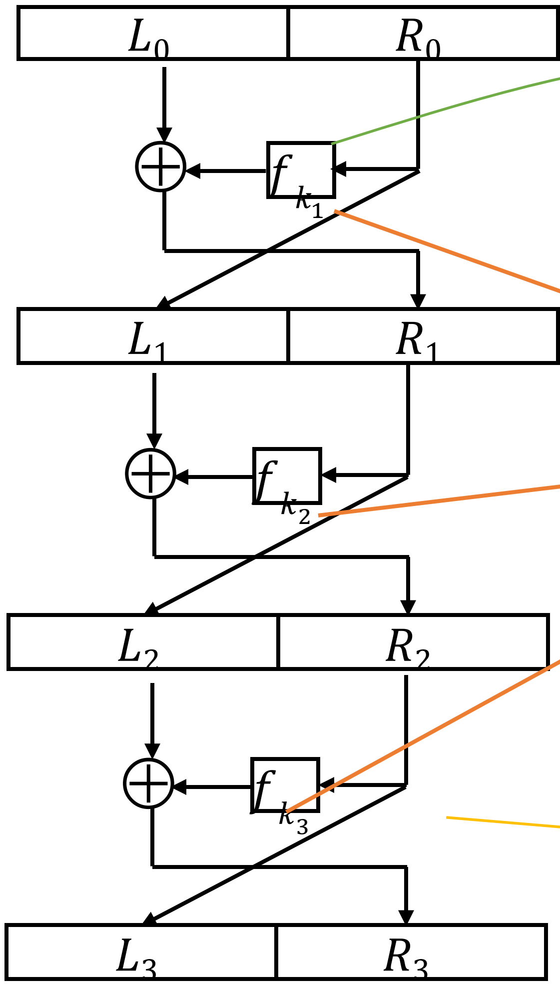
The DES Mangler Function



- S-boxes are designed such that:
  - Each S-box is 4-to-1
  - Changing 1 bit of input changes at least 2 bits of output
- Mixing permutation and E designed such that:
  - The 4 bits of output from any S-box affect the input to 6 S-boxes in the next round
- Each sub-key is derived by taking certain specific 48 bits from the 56-bit master-key. Where left 24 bits are derived from the left 28 bits of master key and right 24 bits are derived from the right 28 bits of the master key.

DES Construction

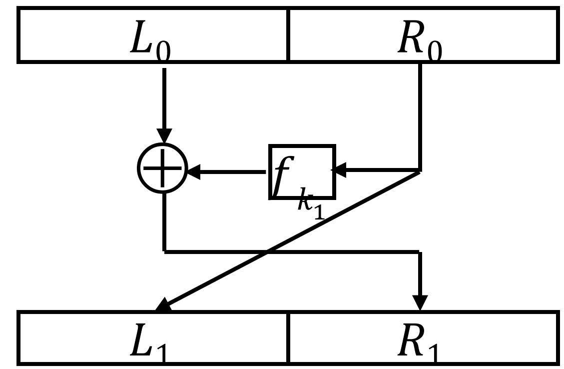




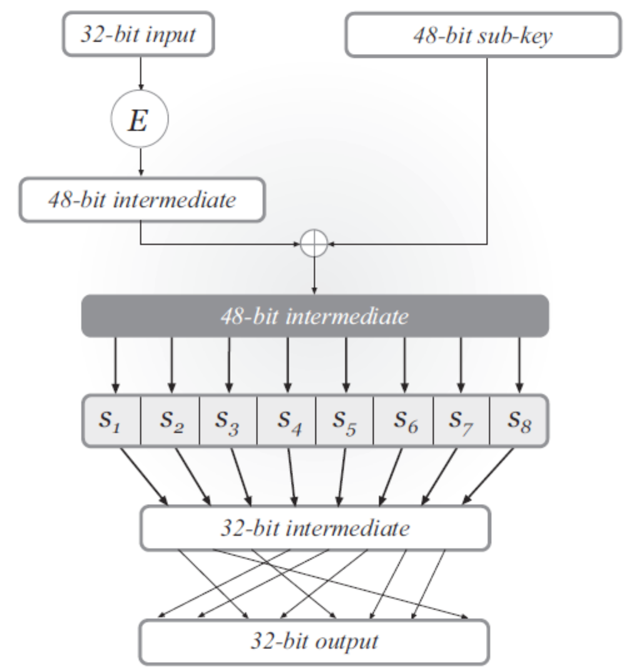
Derived from the 56 bit master key.

Repeated 16 times for Avalanche Effect!

One round DES: Key recovery Attack

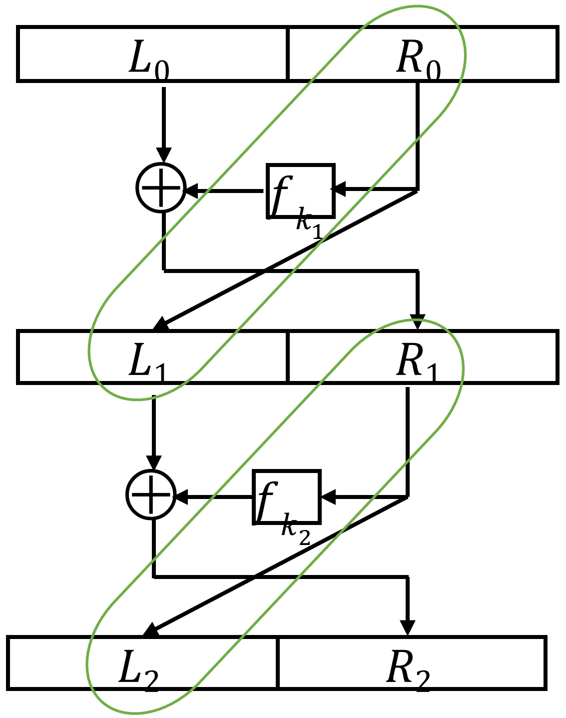


- Observe $f_{k_1}(R_0) = L_0 \oplus R_1$
- Attack similar to SPN
- Recover k_1 by going over each S-box separately
- Total possibilities of key $= 4^8$
  - Using one input/output
- Much smaller than 2^{48}



Two round DES: Key recovery Attack

- Thus, $f_{k_1}(R_0) = L_0 \oplus L_2$ and
  $f_{k_2}(L_2) = R_0 \oplus R_2$
- Obtain k_1 and k_2 as two separate attacks on the DES mangler function.



More Attacks

- Better than brute-force key-recovery attack for three round DES
- Biham and Shamir gave a 2^{37} time attack given 2^{47} plaintexts (considered not practical)

Upgrading Security

- Modify DES to work with larger keys!
  - Risky and error prone!
- Build on DES in a black-box manner

Attempt 1: Double DES

- $F'_{k_1,k_2}(x) = F_{k_2}\left(F_{k_1}(x)\right)$, where k_1 and k_2 are independent keys

- If best attack on F takes time 2^n, then does the best attack on F^2 takes time 2^{2n}?

- No! Still an attack taking 2^n time
  - But, need 2^n memory

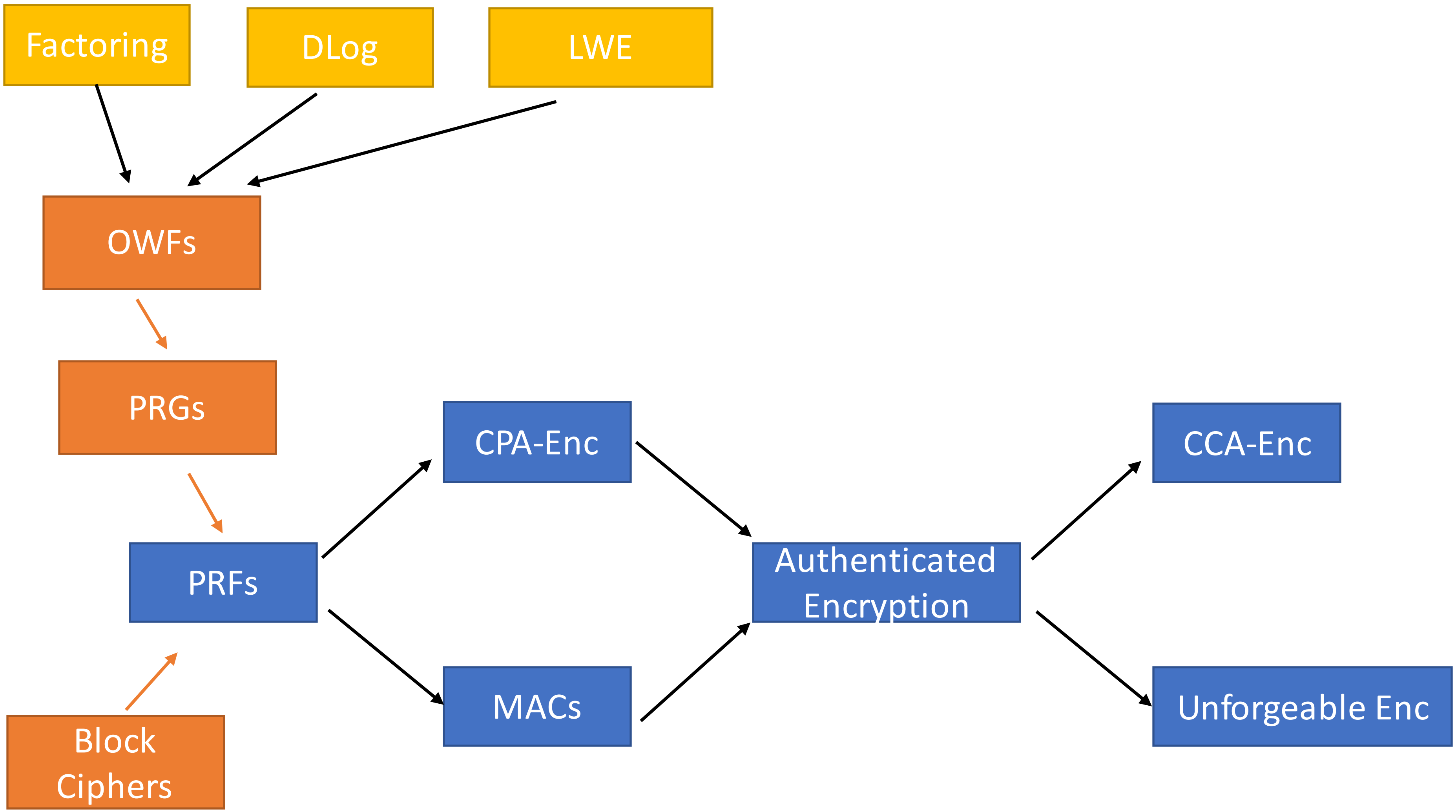
Attack

- Give x, y such that $y = F_{k_2}\left(F_{k_1}(x)\right)$ we have
$$F_{k_2}^{-1}(y) = F_{k_1}(x)$$
- Exhaustively find all k_1, k_2 such that $F_{k_2}^{-1}(y) = F_{k_1}(x)$
- Assuming random behavior - 2^n choices
- Test each with another input/output pair.

Attempt 2: Triple DES

- $F'_{k_1,k_2,k_3}(x) = F_{k_3}(F^{-1}_{k_2}\left(F_{k_1}(x)\right))$, where k_1, k_2 and k_3 are independent keys
- Best attack takes time 2^{2n}
- Now, we have AES (winner announced in 2000).
  - Uses the SPN framework
  - Will not cover in class!

Too Fragile?



Factoring
DLog
LWE
OWFs
PRGs
CPA-Enc
CCA-Enc
PRFs
Authenticated Encryption
MACs
Unforgeable Enc
Block Ciphers

Review

Perfect Security

eav is for Eavesdropper

$\mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi}$

1. A outputs $m_0, m_1 \in \mathcal{M}$.
2. $b \leftarrow \{0,1\}$, $k \leftarrow$ Gen(), $c^* \leftarrow Enc_k(m_b)$
3. c^* is given to A
4. A output b'
5. Output 1 if $b = b'$ and 0 otherwise

Challenge ciphertext

Encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$

is perfectly indistinguishable if

$\forall A$ it holds that:

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi} = 1\right] = \frac{1}{2}$$

A can always succeed with probability ½. How?

Drawback: Large Keys

CPA-Security

$\mathrm{PrivK}^{\mathrm{CPA}}_{A,\Pi}(n)$

1. Sample $k \leftarrow \mathrm{Gen}(1^n)$, $A^{Enc_k(\cdot)}$ outputs $m_0, m_1 \in \{0,1\}^*, |m_0| = |m_1|$.
2. $b \leftarrow \{0,1\}$, $c^* \leftarrow Enc_k(m_b)$
3. c^* is given to $A^{Enc_k(\cdot)}$
4. $A^{Enc_k(\cdot)}$ output b'
5. Output 1 if $b = b'$ and 0 otherwise

Encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions under chosen-plaintext attack, or is *CPA-secure* if

$\forall$ PPT A it holds that:

$$\Pr\left[\mathrm{PrivK}^{\mathrm{CPA}}_{A,\Pi} = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

Only PPT attackers and allowed some failure probability.

Pseudorandom Function (PRF)

Let $F\colon \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, length-preserving, keyed function. F is a PRF if for all PPT distinguishers D, there is a negligible function $negl(\cdot)$ such that:

$$\left|\Pr\left[D^{F_k(\cdot)}(1^n) = 1\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1\right]\right| \leq negl(n)$$

where $k \leftarrow U_n$ and $f \leftarrow Func_n$.

CPA secure Encryption

Let F be a PRF: $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$.

- $Gen(1^n)$: Choose uniform $k \in \{0,1\}^n$ and output it as the key
- $Enc_k(m)$: On input a message $m \in \{0,1\}^n$, sample $r \leftarrow U_n$ output the ciphertext c as
$$c \coloneqq \langle r, F_k(r) \oplus m \rangle$$
- $\mathrm{Dec}_k(c)$: On input a ciphertext $c = \langle r, s \rangle$ output the message
$$m \coloneqq F_k(r) \oplus s$$

Encryption scheme is randomized!

CCA-Security

$\mathrm{PrivK}^{\mathrm{CCA}}_{A,\Pi}(n)$

1. Sample $k \leftarrow \mathrm{Gen}(1^n)$, $A^{Enc_k(\cdot),Dec_k(\cdot)}$ outputs $m_0, m_1 \in \{0,1\}^*$, $|m_0| = |m_1|$.
2. $\mathrm{b} \leftarrow \{0,1\}$, $c^* \leftarrow Enc_k(m_b)$
3. c^* is given $A^{Enc_k(\cdot),Dec_k(\cdot)}$
4. $A^{Enc_k(\cdot),Dec_k(\cdot)}$ (query not allowed on c^*) output b'
5. Output 1 if $b = b'$ and 0 otherwise

Encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions under ciphertext attack, or is *CCA-secure* if

$\forall$ PPT A it holds that:

$$\Pr\left[\mathrm{PrivK}^{\mathrm{CCA}}_{A,\Pi} = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

Will construct in a few lectures!

Good Luck!

Thank You!