Improved Meet-in-the-Middle Attacks on Reduced-Round DES

Orr Dunkelman[1] Gautham Sekar[1] Bart Preneel[1]

[1]Dept. ESAT/SCD-COSIC, K.U.Leuven, Belgium.

Echternach Symmetric Cryptography, January 11, 2008

Outline

Outline

Why Bother?

- We already know how to break the full DES!

Why Bother?

- We already know how to break the full DES!
- We have new, more powerful techniques which made MitM obsolete.

Why Bother?

- We already know how to break the full DES!
- We have new, more powerful techniques which made MitM obsolete.
- We moved to AES!

Motivation

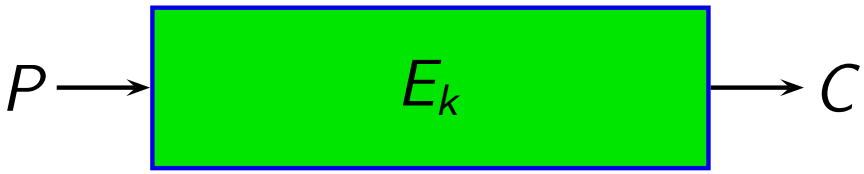
- The retro movements hits Crypto!

Motivation

- The retro movements hits Crypto!
  After seeing 2^{160} chosen plaintext attacks, trying to do stuff with small data complexity.
- Better understanding of some algebraic approaches (optimal sequence of guesses).
- DES-like structure are still in use (and promoted).

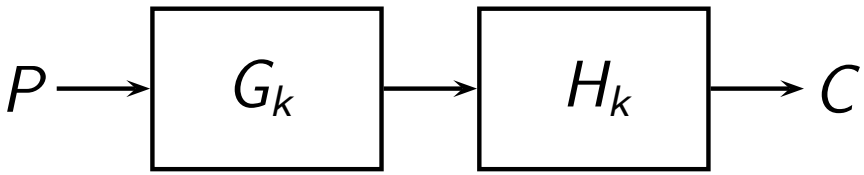
The Basics of Meet in the Middle (MitM) Attacks

- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$



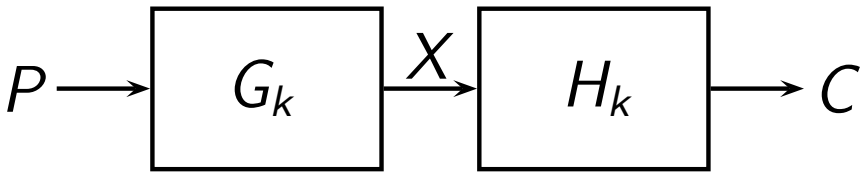
The Basics of Meet in the Middle (MitM) Attacks

- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$



The Basics of Meet in the Middle (MitM) Attacks

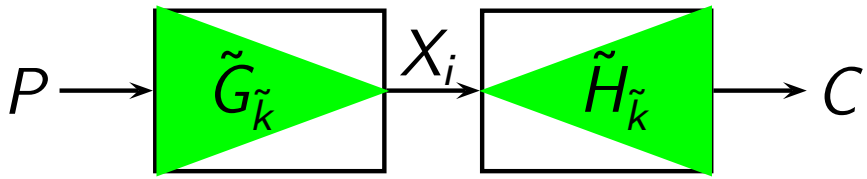
- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$
- Let $C = E_k(P)$, and let $G_k(P) = X = H_k^{-1}(C)$



The Basics of Meet in the Middle (MitM) Attacks

- Consider a block cipher $E_k(\cdot)$ which can be written as $E_k(\cdot) = H_k(\cdot) \circ G_k(\cdot)$
- Let $C = E_k(P)$, and let $G_k(P) = X = H_k^{-1}(C)$
- Assume that a subset of bits i of X can be written as

$$X_i = \tilde{G}_{\tilde{k}}(P)$$
$$X_i = \tilde{H}_{\tilde{k}'}(C)$$

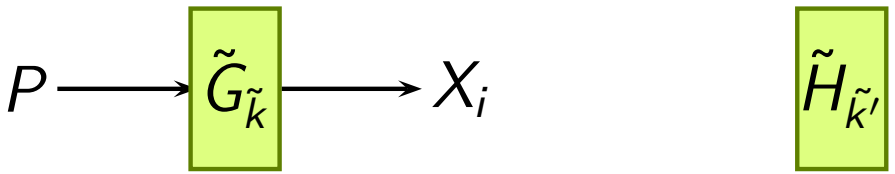


Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, i, \tilde{k}$, and $\tilde{k}'$

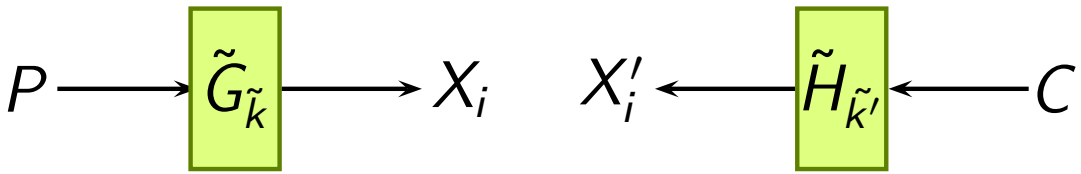
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, i, \tilde{k}$, and $\tilde{k}'$
- Given a plaintext/ciphertext pair (P, C):
  1. For each $\tilde{k}$, compute $X_i = \tilde{G}_{\tilde{k}}(P)$



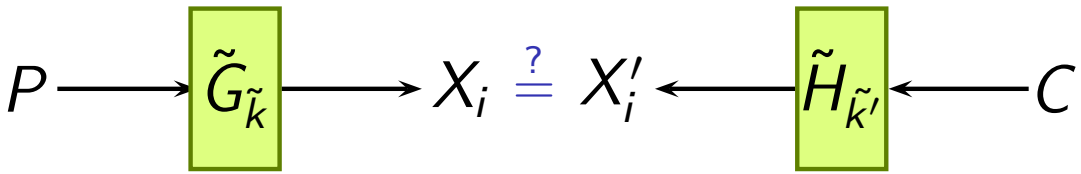
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, i, \tilde{k}$, and $\tilde{k}'$
- Given a plaintext/ciphertext pair (P, C):
  1. For each $\tilde{k}$, compute $X_i = \tilde{G}_{\tilde{k}}(P)$
  2. For each $\tilde{k}'$, compute $X'_i = \tilde{H}_{\tilde{k}'}(C)$



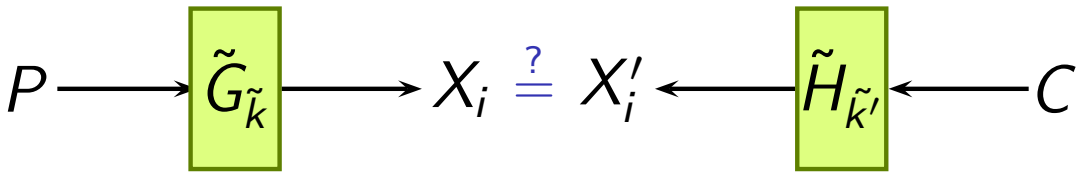
Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, i, \tilde{k}$, and $\tilde{k}'$
- Given a plaintext/ciphertext pair (P, C):
  1. For each $\tilde{k}$, compute $X_i = \tilde{G}_{\tilde{k}}(P)$
  2. For each $\tilde{k}'$, compute $X'_i = \tilde{H}_{\tilde{k}'}(C)$
  3. Only if $X_i = X'_i$ further analyze $\tilde{k}, \tilde{k}'$



Performing a Meet in the Middle Attack

- **Identify** $\tilde{G}, \tilde{H}, i, \tilde{k}$, and $\tilde{k}'$
- Given a plaintext/ciphertext pair (P, C):
  1. For each $\tilde{k}$, compute $X_i = \tilde{G}_{\tilde{k}}(P)$
  2. For each $\tilde{k}'$, compute $X'_i = \tilde{H}_{\tilde{k}'}(C)$
  3. Only if $X_i = X'_i$ further analyze $\tilde{k}, \tilde{k}'$
- Further analyze may be: analyze another plaintext/ciphertext pair, exhaustively search remaining key bits, etc.



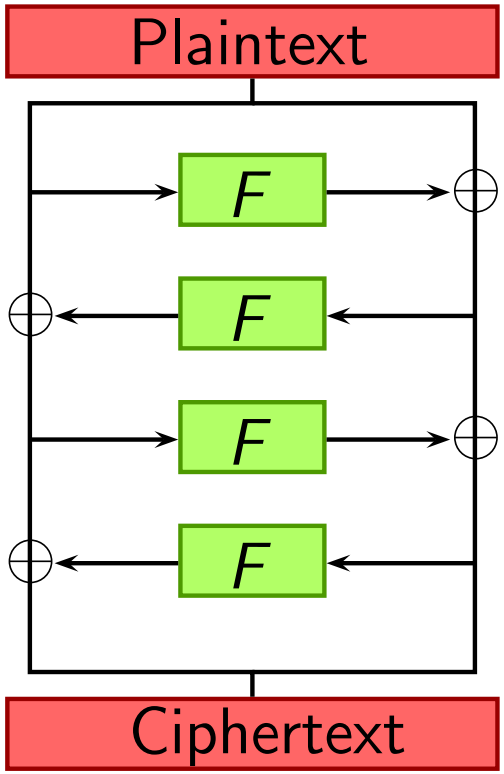
The Data Encryption Standard

- Proposed in mid'70 by IBM to NIST.
- Feistel block cipher with 16 rounds.
- Plaintext/ciphertext size — 64 bits.
- Key size — 56 bits.
- Each round function accepts 48-bit subkey.

Outline

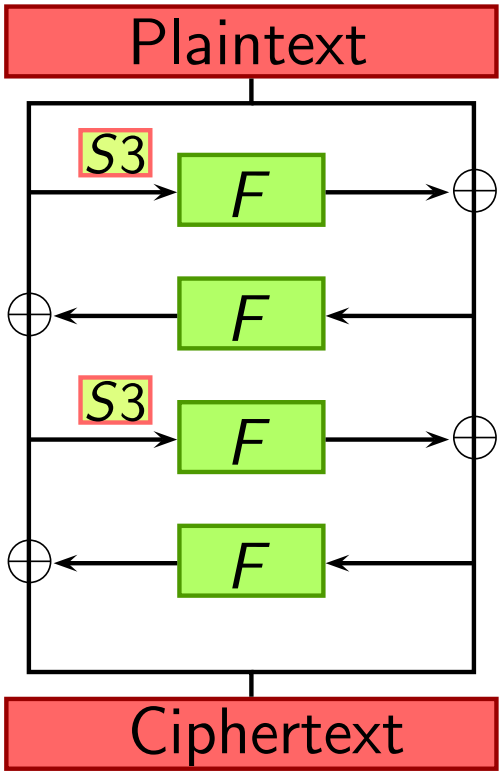
Chaum & Evertse's Attack on DES

- Consider the first four rounds of DES.
- If the attacker knows the output from $S3$ in rounds 1 and 3, he can compute the MitM condition on 4 bits.



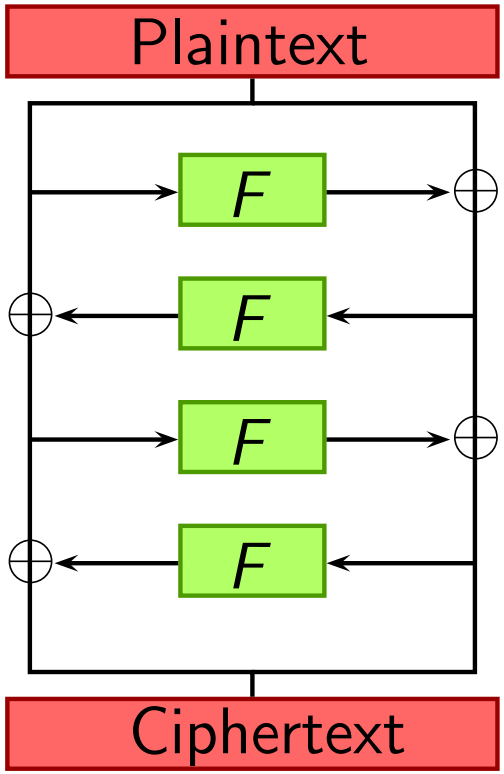
Chaum & Evertse's Attack on DES

- Consider the first four rounds of DES.
- If the attacker knows the output from $S3$ in rounds 1 and 3, he can compute the MitM condition on 4 bits.
- The attacker guesses the subkeys of $R1/S3$ and $R3/S3$.



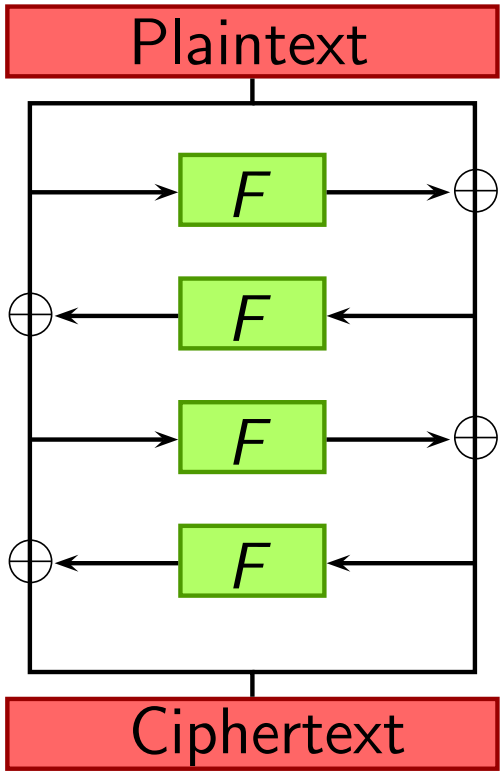
Chaum & Evertse's Attack on DES

- Consider the first four rounds of DES.
- If the attacker knows the output from $S3$ in rounds 1 and 3, he can compute the MitM condition on 4 bits.
- One small problem though...



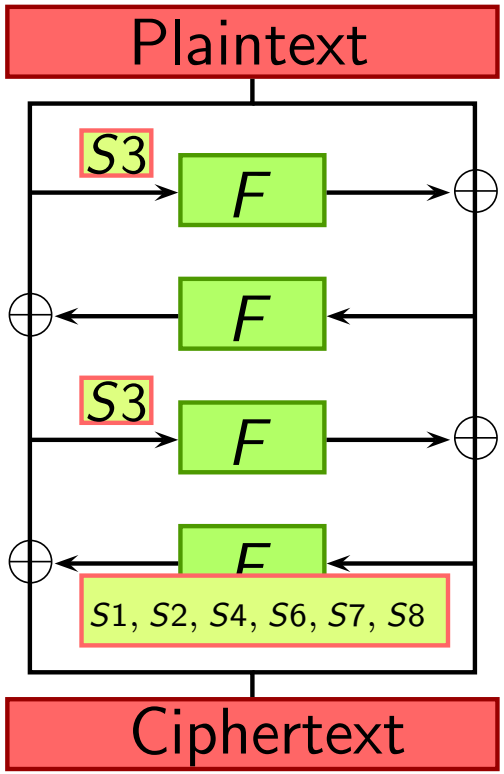
Chaum & Evertse's Attack on DES

- Consider the first four rounds of DES.
- If the attacker knows the output from $S3$ in rounds 1 and 3, he can compute the MitM condition on 4 bits.
- One small problem though... **Guessing the key which enters $R3/S3$ is not sufficient, as the actual input itself is unknown.**



Chaum & Evertse's Attack on DES

- Consider the first four rounds of DES.
- If the attacker knows the output from $S3$ in rounds 1 and 3, he can compute the MitM condition on 4 bits.
- One small problem though... **Guessing the key which enters $R3/S3$ is not sufficient, as the actual input itself is unknown.**
- The attacker has to guess the subkeys of $R4/S1$, $R4/S2$, $R4/S4$, $R4/S6$, $R4/S7$, and $R4/S8$.



Chaum-Evertse's Meet-in-the-Middle Attack on DES (II)

Due to the key schedule, $S1$, $S2$, $S3$, and $S4$ can be directly effected only by 28 key bits.

Chaum-Evertse's Meet-in-the-Middle Attack on DES (II)

Due to the key schedule, $S1$, $S2$, $S3$, and $S4$ can be directly effected only by 28 key bits.

- $R1/S3$ and $R3/3$ share 11 key bits.
- $R4/S1$, $R4/S2$, and $R4/S4$ introduce 8 more bits.

Chaum-Evertse's Meet-in-the-Middle Attack on DES (II)

Due to the key schedule, $S1$, $S2$, $S3$, and $S4$ can be directly effected only by 28 key bits.

- $R1/S3$ and $R3/3$ share 11 key bits.
- $R4/S1$, $R4/S2$, and $R4/S4$ introduce 8 more bits.

We guess 18 more key bits for $R4/S6$, $R4/S7$, and $S4/8$, to obtain three of the bits which enter $R3/S3$.

Outline

The New Approach

Instead of guessing key, we guess internal state bits

The New Approach

Instead of guessing key, we guess internal state bits

- If for a key guess, there is no value of the internal state bits for which the MitM happens — the key is wrong.

The New Approach

Instead of guessing key, we guess internal state bits

- If for a key guess, there is no value of the internal state bits for which the MitM happens — the key is wrong.
- It might be the case that several internal state guesses remain for a given key guess.

The New Approach

Instead of guessing key, we guess internal state bits

- If for a key guess, there is no value of the internal state bits for which the MitM happens — the key is wrong.
- It might be the case that several internal state guesses remain for a given key guess.
- There is a tradeoff between the number of internal state bits which are guessed, and the probability that a wrong key is discarded.

An Attack Procedure Using One Known Plaintext

- For each guess of the 19 key bits,

An Attack Procedure Using One Known Plaintext

- For each guess of the 19 key bits,
  - For each guess of the 3 intermediate key bits, check the MitM on $R3/S3$. If no possible value, discard the key guess.

An Attack Procedure Using One Known Plaintext

- For each guess of the 19 key bits,
  - For each guess of the 3 intermediate key bits, check the MitM on $R3/S3$. If no possible value, discard the key guess.
- Perform MitM on $R3/S2$ (guess 3 more key bits, and check for 4 more intermediate bits).

An Attack Procedure Using One Known Plaintext

- For each guess of the 19 key bits,
  - For each guess of the 3 intermediate key bits, check the MitM on $R3/S3$. If no possible value, discard the key guess.
- Perform MitM on $R3/S2$ (guess 3 more key bits, and check for 4 more intermediate bits).
- Perform MitM on $R2/S1$ (guess 2 more key bits, and check for 4 more intermediate bits).

An Attack Procedure Using One Known Plaintext

- For each guess of the 19 key bits,
  - For each guess of the 3 intermediate key bits, check the MitM on $R3/S3$. If no possible value, discard the key guess.
- Perform MitM on $R3/S2$ (guess 3 more key bits, and check for 4 more intermediate bits).
- Perform MitM on $R2/S1$ (guess 2 more key bits, and check for 4 more intermediate bits).
- ...

An Attack Procedure Using One Known Plaintext

- For each guess of the 19 key bits,
  - For each guess of the 3 intermediate key bits, check the MitM on $R3/S3$. If no possible value, discard the key guess.
- Perform MitM on $R3/S2$ (guess 3 more key bits, and check for 4 more intermediate bits).
- Perform MitM on $R2/S1$ (guess 2 more key bits, and check for 4 more intermediate bits).
- ...
- After finishing the C register, there are about $2^{20.4}$ remaining values.
- Perform MitM on $R2/S8$ (guess 9 more key bits, check for 2 intermediate bits, *verify* two previously guessed intermediate bits).

An Attack Procedure Using Several Known Plaintexts

- It is possible to take several known plaintexts.
- If for any of the known plaintexts the key guess has no "corresponding intermediate bits", the key is wrong.

Guessed Intermediate Bits	Probability to "pass"
1	2^{-3}
2	$2^{-2.1}$
3	$2^{-1.3}$
4	$2^{-0.6}$
5	$2^{-0.2}$
6	$2^{-0.02}$

An Attack Procedure Using Chosen Plaintexts

- By using chosen plaintexts/ciphertexts, it is possible to fix the intermediate bits in all plaintext/ciphertext pairs to the *same* value.

An Attack Procedure Using Chosen Plaintexts

- By using chosen plaintexts/ciphertexts, it is possible to fix the intermediate bits in all plaintext/ciphertext pairs to the *same* value.
- Thus, when a key "passes" the test with some intermediate value(s) for a given plaintext/ciphertext pair, it has to pass the test with *the same* intermediate value(s) for other plaintext/ciphertext pairs.
- This gives a much better filter for discarding wrong subkey guesses (and reduces time complexity significantly).

Outline

Chaum & Evertse's MitM Attack on 5-Round DES

- Guess 6 S-boxes in Round 1: $R1/S1$, $R1/S2$, $R1/S4$, $R1/S5$, $R1/S6$, $R1/S7$.
- Guess $R2/S3$.
- Guess $R4/S3$.
- Guess 6 S-boxes in Round 5: $R5/S1$, $R5/S2$, $R5/S4$, $R5/S5$, $R5/S6$, $R5/S7$.
- Perform MitM on 4 bits.

Number of guessed bits: 47.

Our MitM Attack on 5-Round DES

Observations:

- There are 24 bits used in $R1/S1$, $R1/S2$, $R1/S4$, $R2/S3$, $R4/S3$, $R5/S1$, $R5/S2$, $R5/S4$ — so it's better to guess these.
- There are 23 bits used in $R1/S5$, $R1/S6$, $R1/S7$, $R5/S5$, $R5/S6$, $R5/S7$ which determine only 6 intermediate bits.
- Guessing 6 intermediate bits has a very small chance of discarding wrong key guesses.
- We guess 8 bits more, and then we have to deal with only 4 intermediate bits (two from encryption side and two from decryption side).

Outline

Attacks on 4-Round DES

Attack	Data	Time
Differential	16 CP	Negligible†
Linear	52 KP	$> 2^{13.7}$ †
Algebraic [CB06]	1 KP	2^{46}
MitM [CH85]	1 KP	2^{35} †
MitM	1 KP	$2^{31.2}$
MitM	15 KP	$2^{20.0}$
MitM	6 CC	$2^{19.3}$

Attacks on 5-Round DES

Attack	Data	Time
Differential	64 CP	$> 2^{11.7}$ †
Linear	72 KP	$> 2^{13.8}$ †
Algebraic [CB06]	3 KP	$2^{54.3}$
MitM [CE85]	1 KP	$2^{45.5}$ †
MitM	51 KP	$2^{35.5}$
MitM	28 KP	$2^{37.9}$
MitM	8 CP	2^{30}

Attacks on 6-Round DES

Attack	Data	Time
Differential	256 CP	$2^{13.7}$
Linear	> 104 KP	$2^{13.9}$ †
Algebraic [CB06]	N/A	$2^{50.1}$
MitM [CE85]	1 KP	$2^{52.9}$ †
MitM	1 KP	$2^{51.8}$

Conclusions

- There is a sequence of "good" guesses (which might explain the results of [CB06]).
- MitM might be useful on more rounds than previously believed.

Questions?

Thank you for your attention!

Questions?

Thank you for your attention!

Yes, even those of you reading their emails at this very same moment.

Questions?

Thank you for your attention!

Yes, even those of you reading their emails at this very same moment.

That's OK, I read my emails while you talked.

Questions?

Thank you for your attention!

Yes, even those of you reading their emails at this very same moment.

That's OK, I read my emails while you talked.

Bart, of course I haven't done so during your talk.

Questions?

Thank you for your attention!

Yes, even those of you reading their emails at this very same moment.

That's OK, I read my emails while you talked.

Bart, of course I haven't done so during your talk.

I was just "resting my eyes" a bit