Cryptanalysis
(암호분석)

Chapter 5 – Part 2

2020.5

Contents

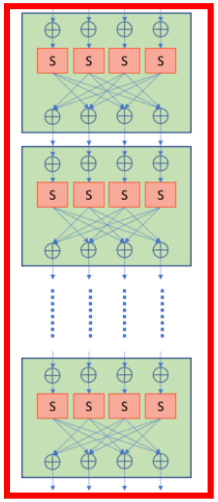
Chapter 5
- Part 1

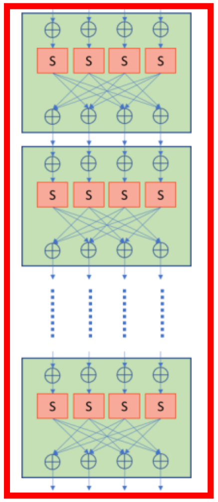
- Generic Attack
- Brute force attack: Exhaustive key search
- Meet-in-the-Middle Attack
- TMTO: Time Memory Trade Off

여기까지
중간고사
범위

- Slide Attack

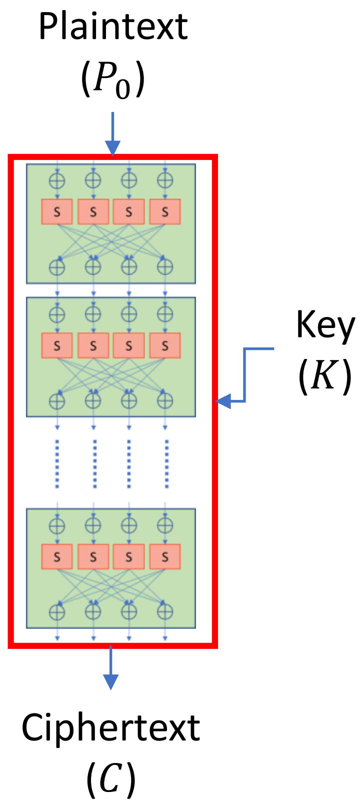
Chapter 5
- Part 3





키 전수조사 공격 유형

- 공격 조건: 선택평문공격(chosen Plaintext Attack)
  - 선택평문(공격자의 선택): P_0
  - 암호문: $C = E(P_0, K)$
  - ➔ 사용된 암호키 (K)를 찾는 공격 $(K \in \{0,1\}^n)$



- 계산 능력에 의존하는 경우(Exhaustive key search)
  - 공격방법: 가능한 2^n 가지의 모든 키를 다 조사해본다.
  - 공격에 사용한 자원: 2^n 계산량

- 저장 능력에 의존하는 경우(Pre-computation)
  - 공격방법: 모든 키에 대하여 $(K, C) = (K, E(\mathrm{P}_0, K))$를 테이블에 저장한 후, 공격대상 암호문$(C)$을 테이블에서 찾는다.
  - 공격에 사용한 자원: 2^n 메모리

Trade-Off

- 두 공격방법의 비교

Table을 만드는 사전계산(Pre-computation) 시간은 공격량에 포함하지 않는다.

	Time(T)	Memory(M)	Attack Complexity
1. Exhaustive Key Search	2^n	1	2^n
2. Table Size	1	2^n	2^n
3. TMTO	▲	■	▲ + ■

$< 2^n$

- 암호 키 공간 $\{0,1\}^n$이 충분히 크면,
  계산시간, 또는 메모리 모두 2^n 능력을 갖기는 어렵다.
- 계산시간, 메모리 자원의 적절한 Trade-Off로 실현 가능한 공격 기법이 있을까?
- 56비트 키를 사용하는 DES의 경우,
  ▲ = ■ = 2^{40} 의 공격법이 있다면, 2^{41}의 공격량으로 해독됨

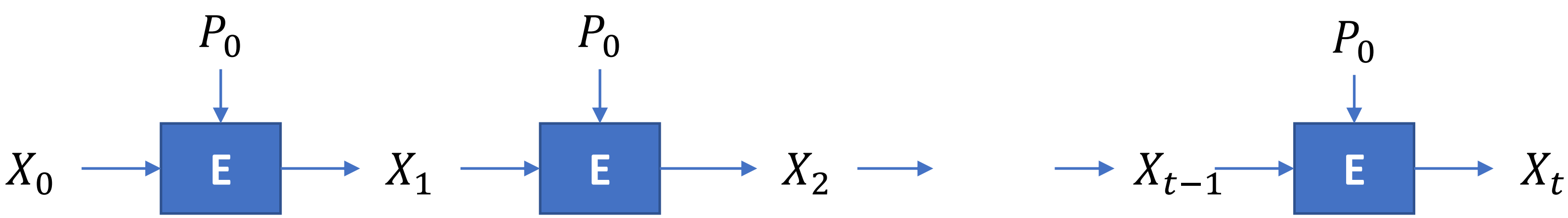
Encryption Chain 구성

- 암호 키 체인의 구성
  - 고정된 선택평문 (P_0) 에 대하여
  - 시작점(X_0): 랜덤하게 선택한 암호 키 $X_0 = K_0$
  - 체인의 계산 규칙: $X_{i+1} = f(X_i)$

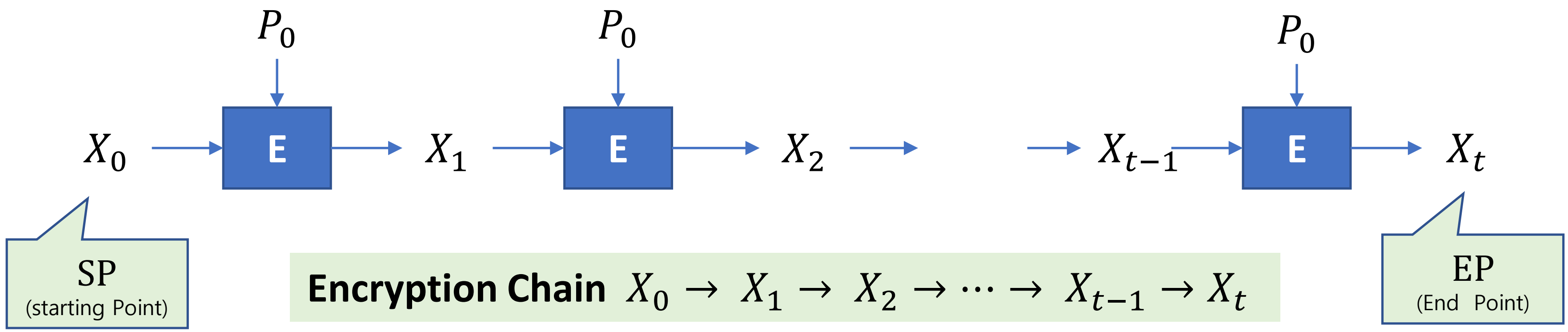
$$f(X_i) = R\big(E(P_0, X_i)\big)$$

    - $E(P_0, X_i)$: 암호 키 X_i로 평문 P_0를 암호화한 결과(암호문)
    - $X_{i+1} = R(C_i)$: 암호문을 암호 키로 변환하는 랜덤 함수

Encryption Chain $X_0 \rightarrow X_1 \rightarrow X_2 \rightarrow \cdots \rightarrow X_{t-1} \rightarrow X_t$



Encryption Chain의 활용(1)



- 체인의 활용 (공격)

$$C = E(P_0, K)$$

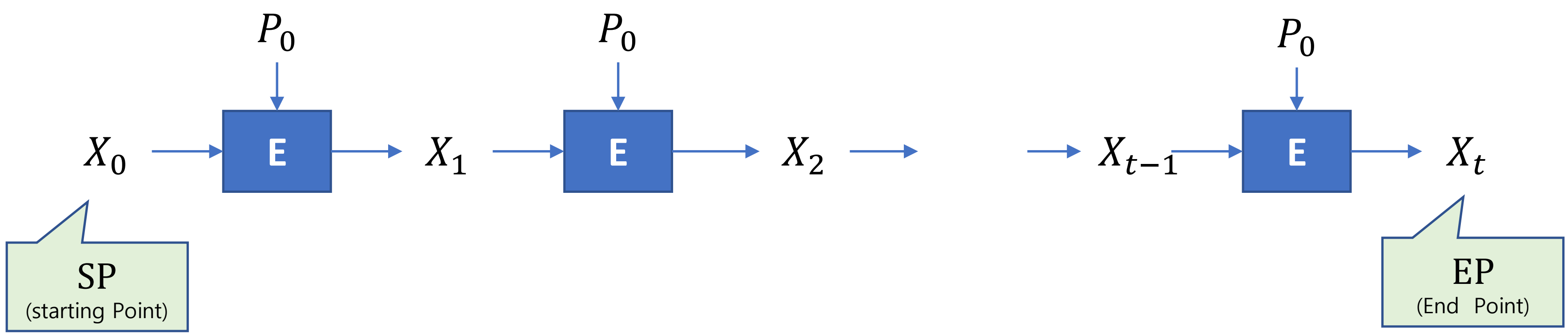
  - 암호문(C) 생성에 사용된 암호 키(K)를 찾는 공격
  - 암호문(C)에 대하여, $R(C) = X_k$ 를 만족한다면,

$$R(\boldsymbol{C}) = X_k = R\big(\boldsymbol{E(P_0, X_{k-1})}\big)$$

  - 암호 키를 X_{k-1}로 판정한다.

암호문과 암호키의
크기가 같다면,
R()을 사용하지 않아도
된다.

Encryption Chain의 활용(2)



- 체인의 시작점(SP)과 끝점(EP)만 저장한다면
  - 암호문(C)에 대하여, $R(C) = X_k$ 를 만족하는 k를 찾기 위해
    $$R(\boldsymbol{C}) = X_k = f(X_{k-1}) = R\left(\boldsymbol{E(P_0, X_{k-1})}\right)$$
  - 체인 길이(t) 만큼의 시도가 필요하다. ($1 \le k \le t$)

Encryption Chain $X_0 \rightarrow X_1 \rightarrow X_2 \rightarrow \cdots \boldsymbol{X_{t-1}} \rightarrow \boldsymbol{X_t} \rightarrow \cdots \rightarrow X_{t-1} \rightarrow X_t$

Hellman 테이블 구성

계산량: $m \times t$
메모리: m

$$
\begin{array}{l}
\mathrm{SP}_1 = X_{1,0} \rightarrow X_{1,1} \rightarrow X_{1,2} \rightarrow \cdots \rightarrow X_{1,t-1} \rightarrow X_{1,t} = \mathrm{EP}_1 \\
\mathrm{SP}_2 = X_{2,0} \rightarrow X_{2,1} \rightarrow X_{2,2} \rightarrow \cdots \rightarrow X_{2,t-1} \rightarrow X_{2,t} = \mathrm{EP}_2 \\
\mathrm{SP}_i = X_{i,0} \rightarrow X_{i,1} \rightarrow X_{i,2} \rightarrow \cdots \rightarrow X_{i,t-1} \rightarrow X_{i,t} = \mathrm{EP}_i \\
\mathrm{SP}_m = X_{m,0} \rightarrow X_{m,1} \rightarrow X_{m,2} \rightarrow \cdots \rightarrow X_{m,t-1} \rightarrow X_{m,t} = \mathrm{EP}_m
\end{array}
$$

- 랜덤하게 m개의 시작점을 선택한다. $\{\mathrm{SP}_1, \mathrm{SP}_2, \dots, \mathrm{SP}_m\}$
- 각 시작점으로 체인을 만든다.

$$\mathrm{SP}_i = X_{i,0} \rightarrow X_{i,1} \rightarrow X_{i,2} \rightarrow \cdots \rightarrow X_{i,t-1} \rightarrow X_{i,t} = \mathrm{EP}_i$$

- 시작점과 끝점만 저장한다.

$$\{(\mathrm{SP}_1, \mathrm{EP}_1), (\mathrm{SP}_2, \mathrm{EP}_2), \dots, (\mathrm{SP}_m, \mathrm{EP}_m)\}$$

- 끝점을 기준으로 정렬(sort)한다.

Hellman 테이블과 키 탐색(1)

$$
\begin{array}{|c|l|c|}
\mathrm{SP}_1 & = X_{1,0} \to X_{1,1} \to X_{1,2} \to \cdots \to X_{1,t-1} \to X_{1,t} = & \mathrm{EP}_1 \\
\mathrm{SP}_2 & = X_{2,0} \to X_{2,1} \to X_{2,2} \to \cdots \to X_{2,t-1} \to X_{2,t} = & \mathrm{EP}_2 \\
\mathrm{SP}_i & = X_{i,0} \to X_{i,1} \to X_{i,2} \to \cdots \to X_{i,t-1} \to \color{red}{\boldsymbol{X_{i,t}}} = & \mathrm{EP}_i \\
\mathrm{SP}_m & = X_{m,0} \to X_{m,1} \to X_{m,2} \to \cdots \to X_{m,t-1} \to X_{m,t} = & \mathrm{EP}_m
\end{array}
$$

- 암호 키 탐색
  - 암호문(C)이 $R(C) = \mathrm{EP}_i$ 를 만족한다면,

    $$R(\color{red}{\boldsymbol{C}}) = X_t = R\left(\color{red}{\boldsymbol{E(P_0, X_{t-1})}}\right)$$
  - 암호 키를 X_{t-1}로 판정한다.

Hellman 테이블과 키 탐색(2)

$$
\begin{array}{lcl}
\mathrm{SP}_1 & = X_{1,0} \to X_{1,1} \to \cdots \quad X_{1,s} \to X_{1,s+1} \to \cdots \to X_{1,t-1} \to X_{1,t} = & \mathrm{EP}_1 \\
\mathrm{SP}_2 & = X_{2,0} \to X_{2,1} \to \cdots \quad X_{2,s} \to X_{2,s+1} \to \cdots \to X_{2,t-1} \to X_{2,t} = & \mathrm{EP}_2 \\
\mathrm{SP}_i & = X_{i,0} \to X_{i,1} \to \cdots \quad \boldsymbol{X_{i,s}} \to \boldsymbol{X_{i,s+1}} \to \cdots \to \boldsymbol{X_{i,t-1}} \to \boldsymbol{X_{i,t}} = & \mathrm{EP}_i \\
\mathrm{SP}_m & = X_{m,0} \to X_{m,1} \to \cdots \quad X_{m,s} \to X_{m,s+1} \to \cdots \to X_{m,t-1} \to X_{m,t} = & \mathrm{EP}_m
\end{array}
$$

- 암호 키 탐색
  - 암호문(C)이 $R(C) = \mathrm{EP}_i$ 를 만족한다면, 암호 키를 $X_{i,t-1}$로 판정한다.

    $$R(\boldsymbol{C}) = X_{i,t} = f\left(X_{i,t-1}\right) = R\left(\boldsymbol{E}\left(\boldsymbol{P_0}, \boldsymbol{X_{i,t-1}}\right)\right)$$

  - 같은 원리로 암호문이 다음을 만족하면 암호키를 $X_{i,s-1}$로 판정한다.

    $$f^{t-s}(R(C)) = \mathrm{EP}_i$$

Hellman 테이블과 키 탐색(3)

$$
\begin{array}{lcl}
\mathrm{SP}_1 & = & X_{1,0} \rightarrow X_{1,1} \rightarrow X_{1,2} \rightarrow \cdots \rightarrow X_{1,t-1} \rightarrow X_{1,t} = \mathrm{EP}_1 \\
\mathrm{SP}_2 & = & X_{2,0} \rightarrow X_{2,1} \rightarrow X_{2,2} \rightarrow \cdots \rightarrow X_{2,t-1} \rightarrow X_{2,t} = \mathrm{EP}_2 \\
\mathrm{SP}_i & = & X_{i,0} \rightarrow X_{i,1} \rightarrow X_{i,2} \rightarrow \cdots \rightarrow X_{i,t-1} \rightarrow X_{i,t} = \mathrm{EP}_i \\
\mathrm{SP}_m & = & X_{m,0} \rightarrow X_{m,1} \rightarrow X_{m,2} \rightarrow \cdots \rightarrow X_{m,t-1} \rightarrow X_{m,t} = \mathrm{EP}_m
\end{array}
$$

$m \times t$ 행렬
(각 원소에
하나의 키
후보가 대응됨)

- (매우 낙관적인) 공격 방법
  - 암호문(C)에 대하여 $R(C) = \mathrm{EP}_i$를 만족하는 끝점이 있는지 찾는다.
  - 없으면 $f\big(R(C)\big) = \mathrm{EP}_i$를 만족하는 끝점을 찾는다.
  - 반복하여 $f^2\big(R(C)\big), f^3\big(R(C)\big), \ldots$ 중 EP_i와 같은 것이 있는지 계속한다.

➔ 각 점은 $R\left(\boldsymbol{E}\left(\boldsymbol{P}_0, \boldsymbol{X}_{i,j}\right)\right)$ 암호키 $\boldsymbol{X}_{i,j}$ 로 고정된 평문 P_0 를 암호화한 것으로,
키 공간 만큼 큰 테이블이 모든 암호키를 포함하고 있으면 공격이 가능하다.

키 탐색 공격의 문제점(1)

- 탐색공간 문제: 테이블의 포함된 암호키가 충분한가?
  - 체인 구성에 사용된 함수 f가 랜덤하다고 가정하자.
  - 테이블의 크기 $(m \times t)$를 어떻게 하는 것이 적절한가?

$m \times t$ 행렬
(각 원소에
하나의 키
후보가 대응됨)

$$\begin{aligned}
\mathrm{SP}_1 &= X_{1,0} \rightarrow X_{1,1} \rightarrow X_{1,2} \rightarrow \cdots \rightarrow X_{1,t-1} \rightarrow X_{1,t} = \mathrm{EP}_1 \\
\mathrm{SP}_2 &= X_{2,0} \rightarrow X_{2,1} \rightarrow X_{2,2} \rightarrow \cdots \rightarrow X_{2,t-1} \rightarrow X_{2,t} = \mathrm{EP}_2 \\
\mathrm{SP}_i &= X_{i,0} \rightarrow X_{i,1} \rightarrow X_{i,2} \rightarrow \cdots \rightarrow X_{i,t-1} \rightarrow X_{i,t} = \mathrm{EP}_i \\
\mathrm{SP}_m &= X_{m,0} \rightarrow X_{m,1} \rightarrow X_{m,2} \rightarrow \cdots \rightarrow X_{m,t-1} \rightarrow X_{m,t} = \mathrm{EP}_m
\end{aligned}$$

암호키의 종류가
2^N 개 라고 하자.
(키 공간 = n 비트)

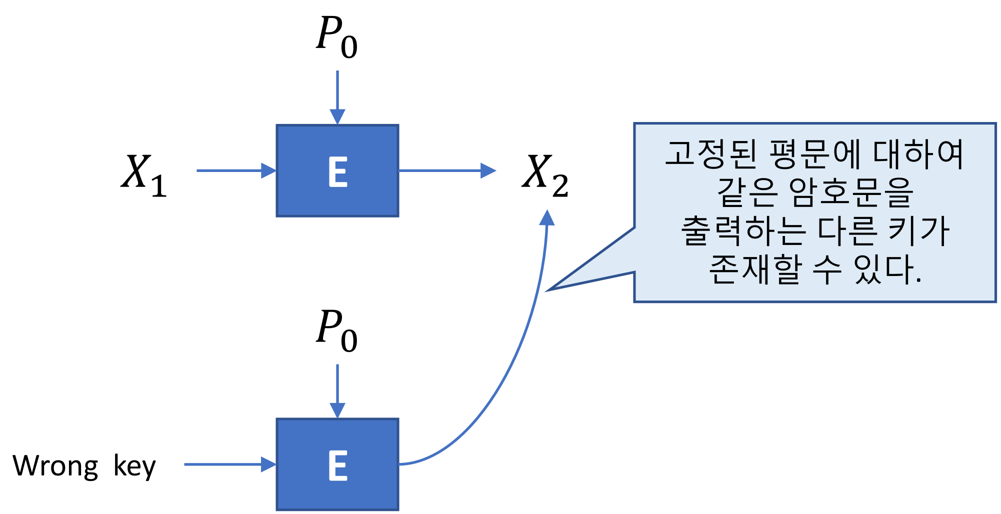
- 테이블의 모든 값이 다르다면 각각 다른 키를 추천하므로,
  $mt = 2^n$ 이면 항상 키 복구가 가능할 것으로 기대됨

→ 확률계산을 통해 분석해보면, 불가능한 시나리오 임 !!!

키 탐색 공격의 문제점(2)

- False Alarm 문제: 잘못된 키가 추천될 가능성과 이를 걸러내는 방법은?
  - 판별식 $f^{t-s}(R(C)) = \mathrm{EP}_i$ 에서 다음 식을 우연히 만족하는 $\boldsymbol{X_{i,s-1}}$ 가 추천되었을 가능성은?

$$R(\boldsymbol{C}) = X_{i,s} = f(X_{i,s-1}) = R\left(\boldsymbol{E}(\boldsymbol{P_0}, \boldsymbol{X_{i,s-1}})\right)$$



→ 다른 평문에 대한 암호문을 비교하는 방법으로 wrong key를 걸러내면 된다

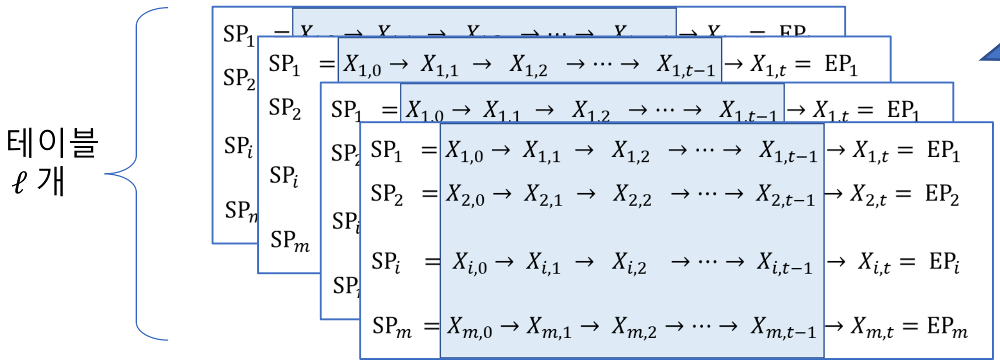
테이블 분석

- ECR: Expected Coverage Rate
  - 암호 알고리즘이 랜덤하다고 가정하자.
  - 테이블 구성에 사용된 $X_{i,j}$ 가 모두 랜덤하게 선택된다고 생각할 수 있다.
  - $\mathrm{ECR}(N,m,t) = \dfrac{\overline{H}}{mt}$, $\overline{H} = \{X_{i,j} \mid 1 \le i \le m, 0 \le j < t\}$

$\overline{H} = mt$ 라면 $ECR = 1$.
(모두 다른 값)
하지만, 실제로 ECR은
경우에 따라 다르며
크지 않다.

$$
\begin{array}{llllll}
\mathrm{SP}_1 & = \boxed{X_{1,0} \to X_{1,1} \to X_{1,2} \to \cdots \to X_{1,t-1}} & \to X_{1,t} = \mathrm{EP}_1 \\
\mathrm{SP}_2 & = X_{2,0} \to X_{2,1} \to X_{2,2} \to \cdots \to X_{2,t-1} & \to X_{2,t} = \mathrm{EP}_2 \\
\mathrm{SP}_i & = X_{i,0} \to X_{i,1} \to X_{i,2} \to \cdots \to X_{i,t-1} & \to X_{i,t} = \mathrm{EP}_i \\
\mathrm{SP}_m & = X_{m,0} \to X_{m,1} \to X_{m,2} \to \cdots \to X_{m,t-1} & \to X_{m,t} = \mathrm{EP}_m
\end{array}
$$

TMTO 공격 성공 확률



$m \times t$ 행렬
(각 원소에
하나의 키
후보가 대응됨)

- Hellman 테이블 ℓ 개를 이용한 TMTO 공격의 성공 확률 (암호 키 공간: $N = 2^n$)

$$P(S) = 1 - \underbrace{\left(1 - \overbrace{\mathrm{ECR}\frac{mt}{N}}^{\text{하나의 테이블에서 암호 키가 발견될 확률}}\right)^{\ell}}_{\text{모든 테이블에서 암호 키가 발견되지 않을 확률}} \approx 1 - \exp\left(-\frac{\ell mt\ \mathrm{ECR}}{N}\right)$$

다음 시간에…

- TMTO 확률 계산
  - TMTO 공격의 성공확률
  - 최적의 파라미터 선택
  - 공격의 개선 방향

- 중간고사 범위는 이번 슬라이드까지 입니다

Good Luck to All !