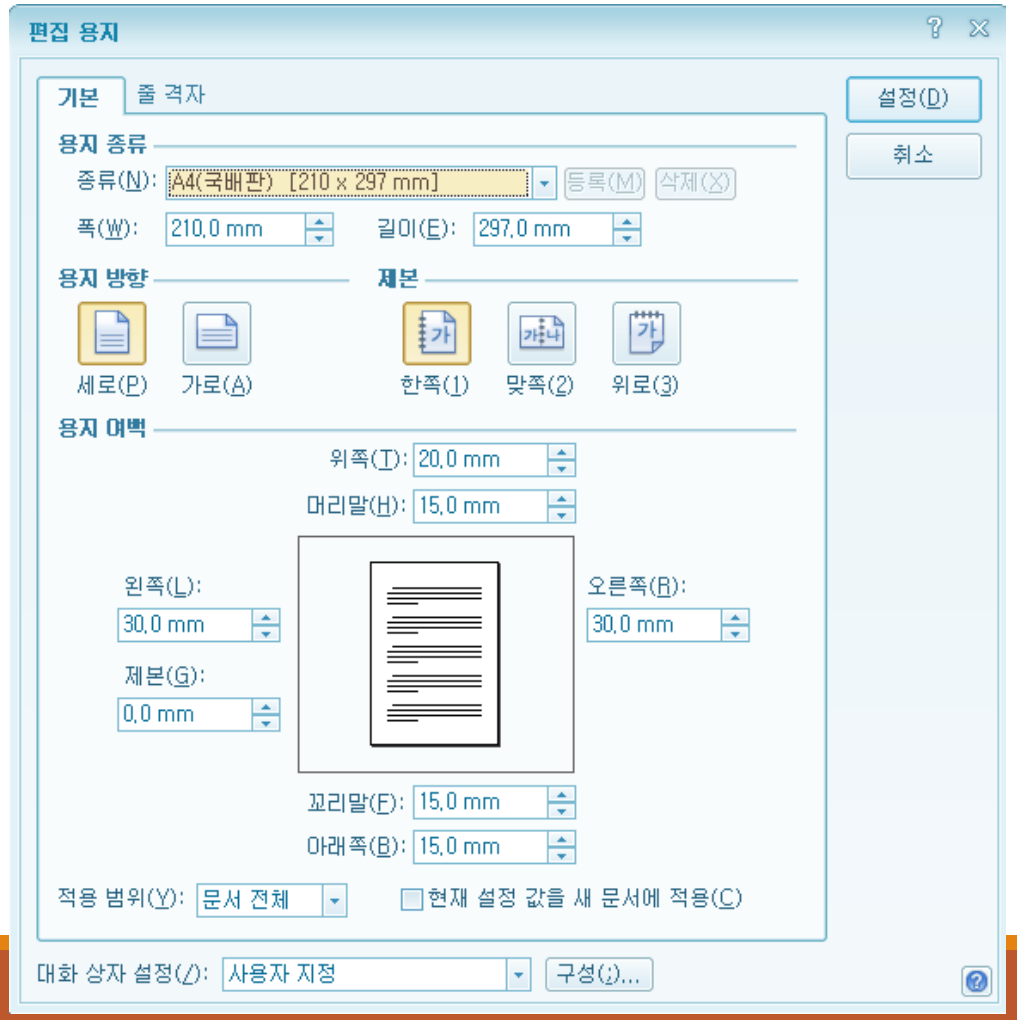
한글 1회차

편집 용지 설정 및 다단 설정

목차

- 편집 용지 설정
- 다단 설정

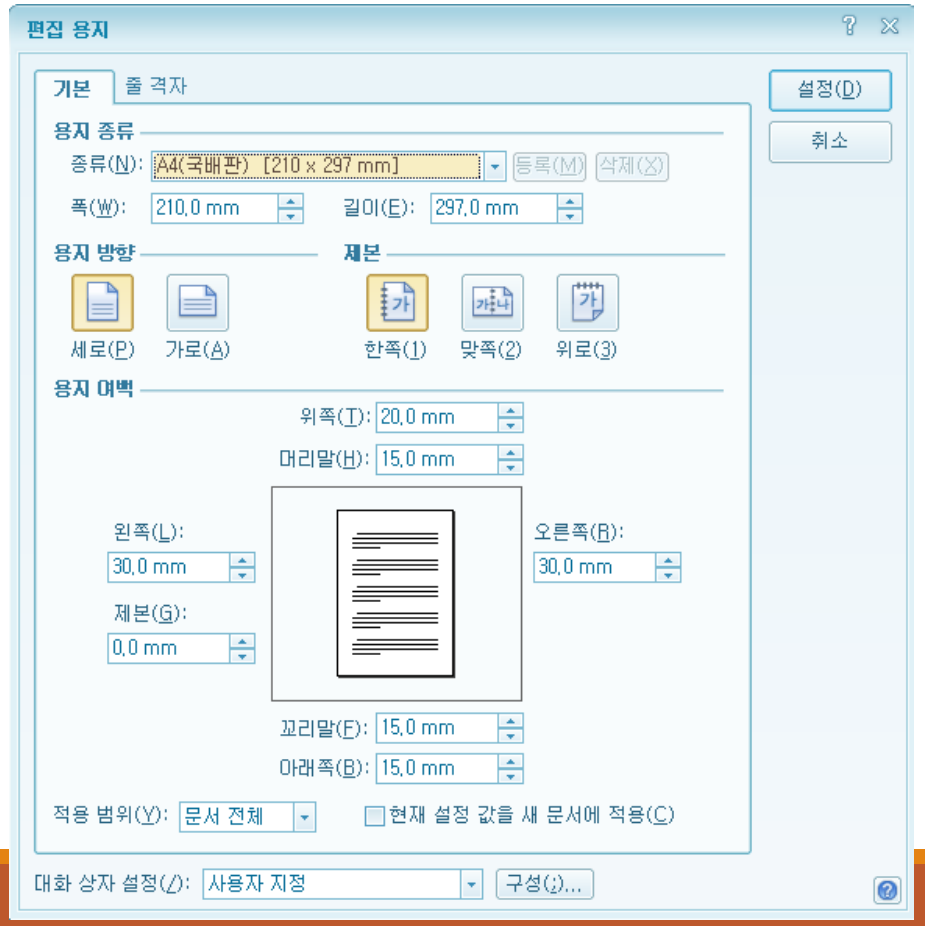
편집 용지 들어가기

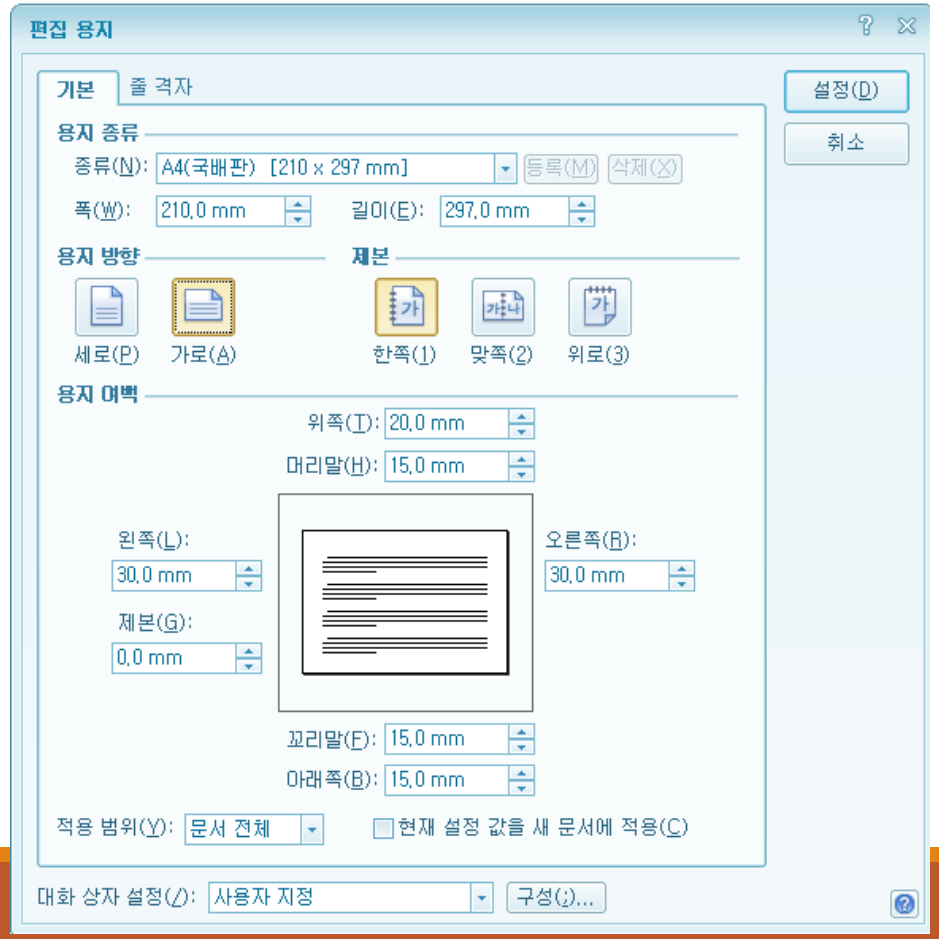


키보드 F7 으로 간단하게 !

편집 용지 - 용지방향

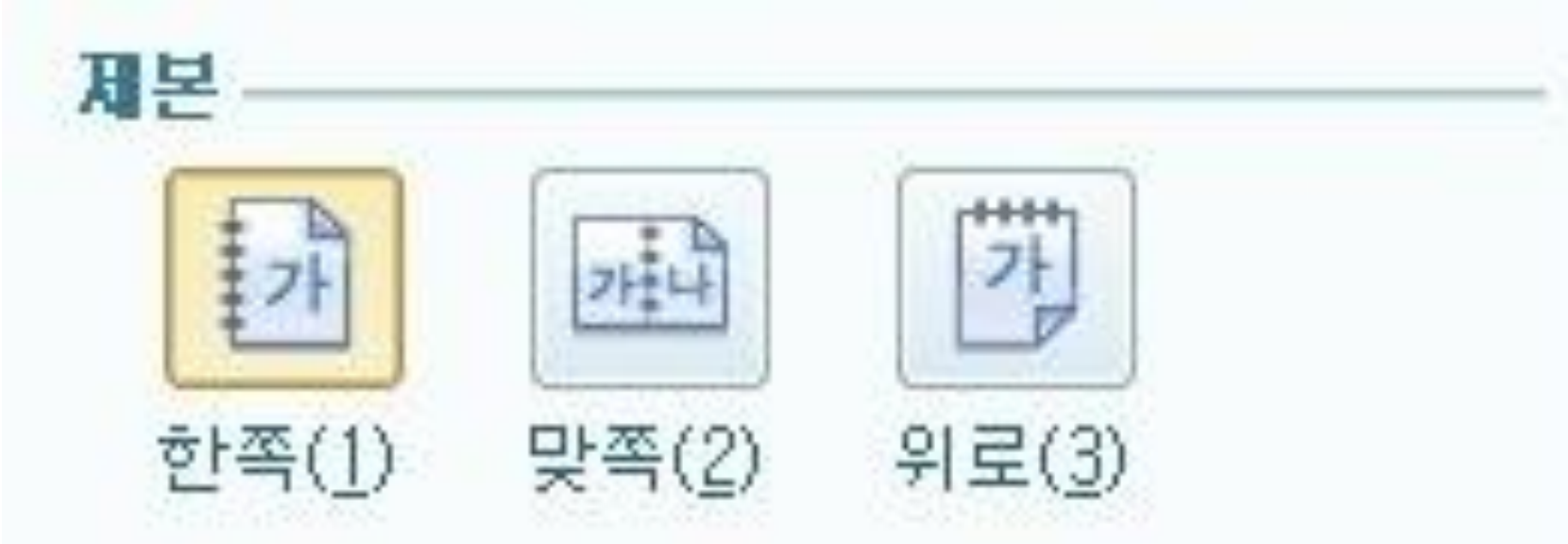
용지의 프린트 방향 설정 가능



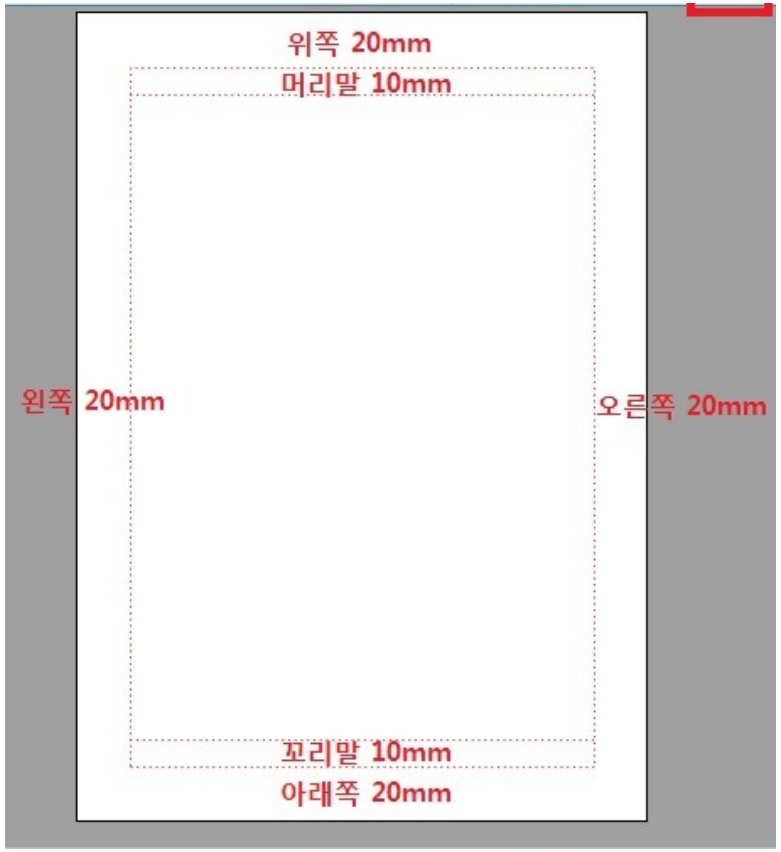


편집 용지 - 제책

제본 할 때 지면의 방향을 설정

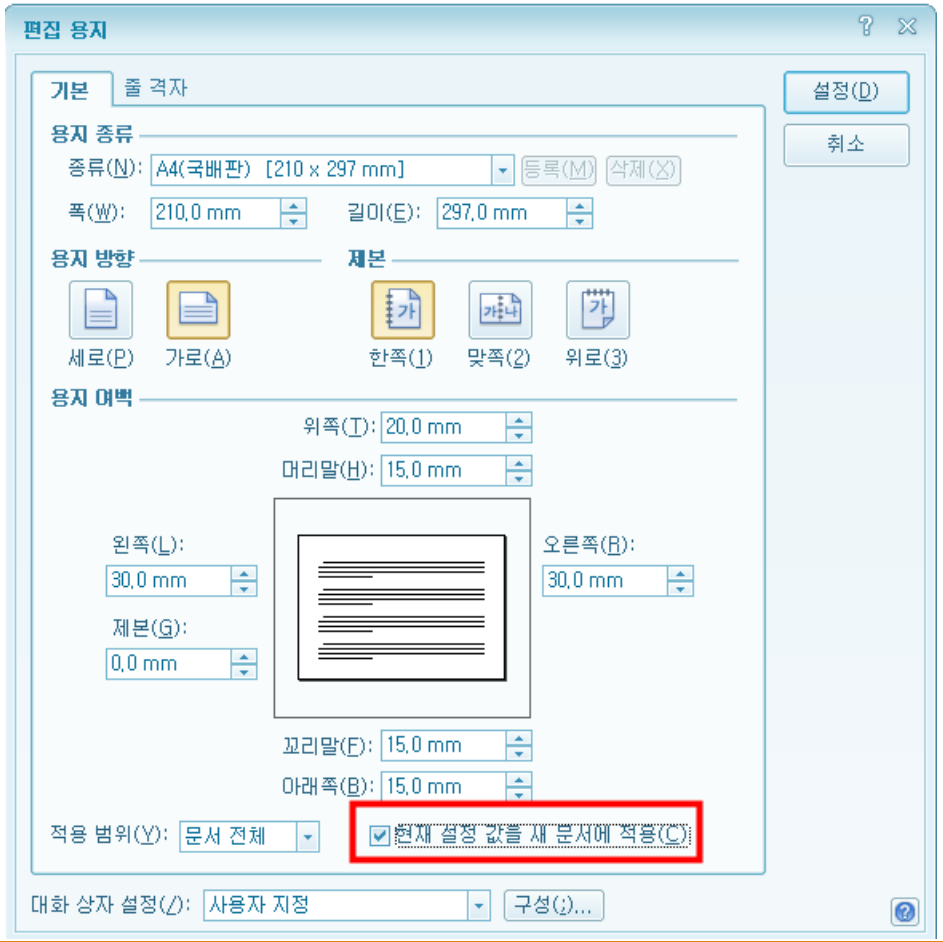


편집용지 - 용지여백



- 사진과 같이 여백을 설정할 수 있음
- 메인메뉴 -> 파일(F) -> 미리보기(V) 에서 여백보기를 클릭하면 현재 문서의 여백 설정을 볼 수 있음
- 값 설정 시 Tab 키를 누르면 빠르게 이동 가능

편집용지 – 설정 유지



해당 환경설정을 새 문서 열 때도 적용하려면 체크!

불필요한 반복 작업을 할 필요 없음!

다단 설정

SNORT 규칙 분석을 통한 새로운 규칙 생성

심항섭 배준우 박희진
한양대학교 한양대학교 한양대학교
컴퓨터공학부 전자컴퓨터통신공학과 컴퓨터공학부
simhs93@naver.com zzale@hanyang.ac.kr hjpark@hanyang.ac.kr

Generate Extended Snort Rules by Edit Distance

Hangseob Sim[1] Junwoo Bae[2] Heejin Park[1]
[1] Department of Computer Science and Engineering, Hanyang University
[2] Department of Electronics and Engineering, Hanyang University

요 약

Snort 란 실시간 트래픽 분석과 ip 네트워크 상에서 패킷 logging 이 가능한 네트워크 침입 탐지 시스템으로 미리 정해진 규칙을 기반으로 탐지 활동을 진행한다. Snort에서는 Packet을 검사하기 위한 rule을 사용하고 있으며, 본 논문의 목적은 기존에 제공되는 Snort 규칙으로부터 향후 발생할 수 있는 새로운 규칙을 도출하고 이를 통해 다른 유형의 네트워크 패킷 공격을 탐지하는 것이다. 이를 위해 기존의 rule 들을 비교 및 분석하여 변형 패턴을 도출한 후 이를 다른 규칙들에 적용하여 새로운 탐지 규칙을 생성한다.

1. 서 론

Snort는 네트워크 상에서 전송되는 패킷 중에 악의적인 공격을 포착하고 이를 방어해내는 시스템이다[1]. Snort의 구성은 크게 스니퍼, 전처리기, 탐색엔진, 로깅이며 그 중 탐색엔진에서 악성 패킷을 탐지할 때 사용되는 것이 규칙(Rule)이다.

Snort 에서 제공되는 규칙은 크게 Rule Header 와 Rule Option 으로 나뉘어진다. 그 중 패킷을 분석하는데 필요한 정보는 Rule Option에 담겨있는데 이를 PCRE(Perl Compatible Regular Expressions)라 부른다. PCRE를 통해 네트워크 패킷에서 탐지해낼 패킷에 대한 표기가 가능한데 본 연구는 2016년 2월달 기준 Snort 규칙 세트로부터 793개의 PCRE를 추출하였다. 이렇게 추출된 규칙들은 유사한 변형을 포함한다는 기존 연구결과가 존재하며[2] 이를 위해 각 규칙을 다른 규칙들과 Edit Distance[3] 수치를 이용해서 이와 유사한 다른 규칙 패턴들을 도출해낸다. 그 후 도출한 규칙간에 어떤 변화점이 있는지 찾아낸 후 이를 다른 규칙에 적용함으로써 새로운 PCRE를 보유하는 규칙을 이끌어낸다. 이로써 향후 아직 정립되지 않은 새로운 네트워크 공격을 방어하는 것이 이 본 논문의 목표이다.

본 논문의 구성은 다음과 같다. 2장은 전체적인 연구 과정을 개발 논리 및 과정 기준으로 나누어 설명한다. 2.1절로는 연구의 개발환경, 2.2절은 PCRE의 추출, 2.3은 Edit Distance 의 기본 개념 2.4는 최종적으로 어떻게 새로운 규칙을 도출해내는지 설명한다. 3장은 본 논문의 결론 및 향후에 영향을 끼칠 수 있는 시사점에 대해 설명한다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW중심대학지원사업 (IITP-2016-R7719-16-1003)의 연구결과로 수행되었음.

2. 연구 과정

2.1 개 발 환 경

개발 환경은 Microsoft 사의 Visual Studio 2015 Community 이란 IDE 툴을 썼고 C++ 을 이용하여 규칙들을 분석하였다.

2.2 PCRE 추 출

Snort 공식 홈페이지에서 제공하는 기존 규칙들(2016년 2월 기준)로부터 PCRE를 추출하며 그 개수는 793개이다.

규칙마다 Rule Header와 Rule Option 으로 구성이 되어 있는데 그 중 Rule Option 부분에서 표현되는 PCRE 부분을 추출해낸다

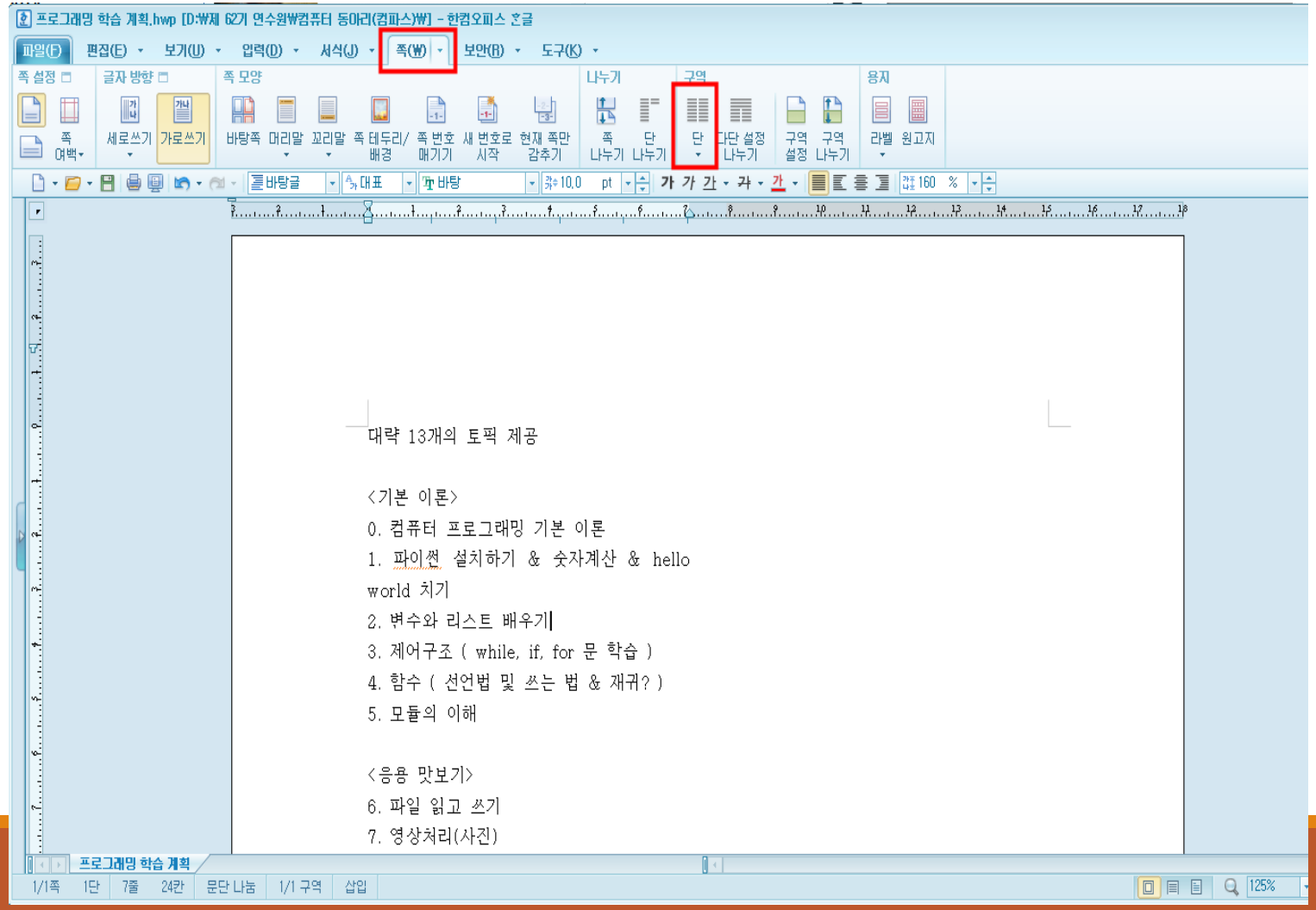
2.3 Edit Distance Algorithm

추출한 PCRE 각각에 대해 가장 유사한 정도로 다른 PCRE를 선발한다. 이 때 Edit Distance란 두 문자열간 하나의 문자열을 다른 문자열로 변환하기 위해 요구되는 연산의 수를 의미한다. 연산은 변환, 삽입, 삭제 3가지가 있다. 두 문자열 각각 x[1..m], y[1..n] 이라 할 때 D(I,J)는 x[1..I] 와 y[1..J] 의 Edit Distance 라 정의하고 이는 재귀적으로 min(D(I-1,J)+1 , D(I,J-1) + 1 , D(I-1,J-1) + Q(I,J)) 로 표현된다. 이 때 Q(I,J)는 match 시 0 , change 시 1 이다.

하나의 페이지를 여러 개로 나누고 싶을 때 다단 설정

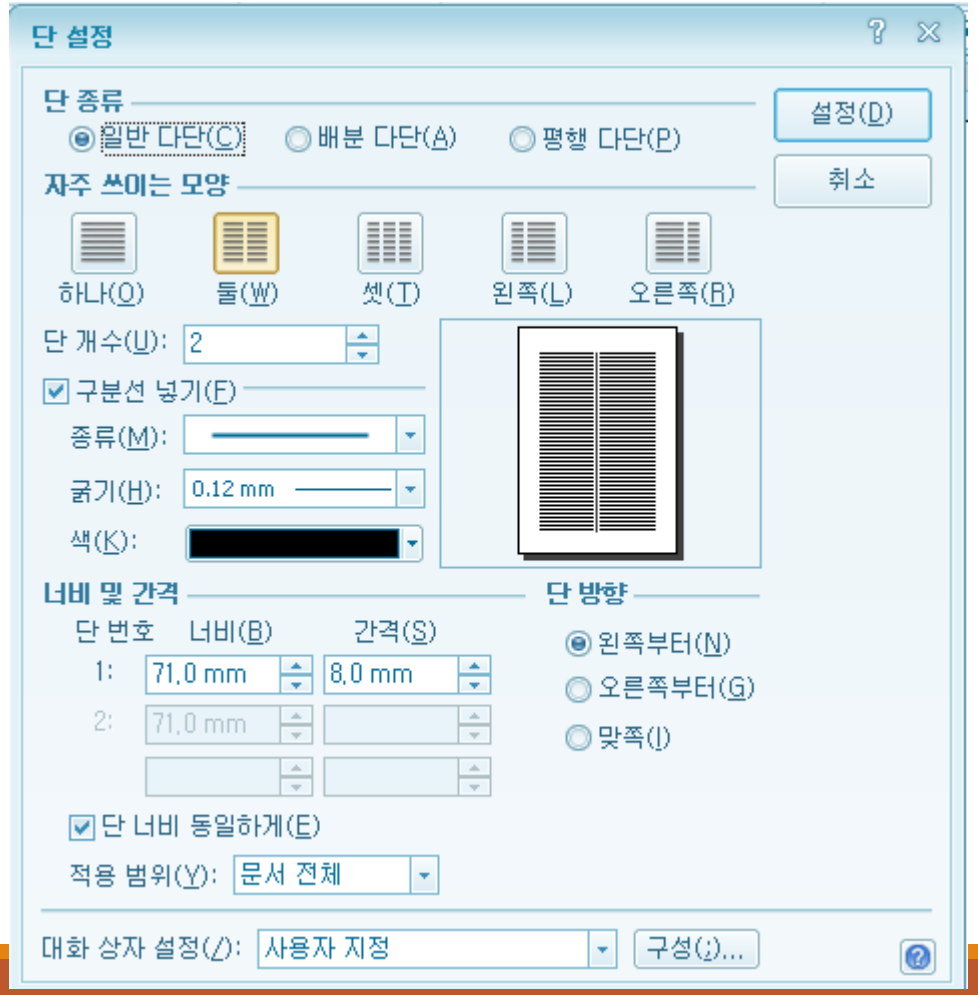
(보통 2단 편집을 함)

다단 설정 – 2단 나누기



조그만 화살표 클릭해 간단하게 몇 단으로 할 지 선택 가능

다단 설정 – 세부



- 단 버튼 클릭시 세부적인 단 설정 가능
  -> 단축키 (Alt + W 후 U)
- 구분선 설정으로 중간에 선으로 구분 가능

실습

https://github.com/SIMHANGSUB/CodingParty62 의 SIM - 한글 -1회차 에 있는 1회차 과제.hwp 문서 수정하고 자신의 폴더에 수정본 올리기!

1. 용지 여백 위쪽 · 아래쪽 · 왼쪽 · 오른쪽 각각 20mm, 머리말 · 꼬리말은 10mm, 기타 여백은 0mm로 지정하기

2. 문서 본문을 2단으로 편집 및 실선 0.12mm짜리 구분선 설정하기