Metamorphic Test 이론

커피동아리 권혁동

Metamorphic Test란?

Bit-Contribution Test

Bit-Exclusion Test

Update Test

Metamorphic Test란?

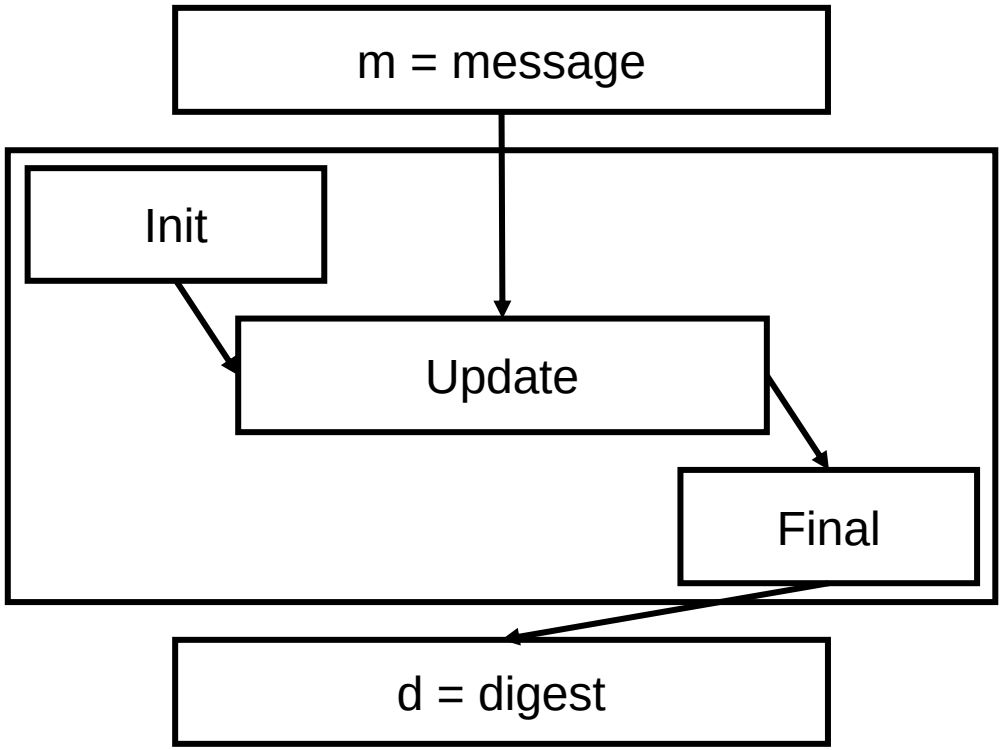
- 기존 암호 구현 적합성 테스트는 테스트 벡터의 일치만 확인
  - 운용모드 구분이 아닌 다양한 테스트 방법이 존재
  - KAT: Known Answer Test, 정형화된 키, 평문을 사용하는 테스트
  - MCT: Monte Carlo Test, 반복적인 동작의 정확성을 테스트
  - MMT: Multi-block Message Test, 블록이 길이를 다양하게 하여 테스트

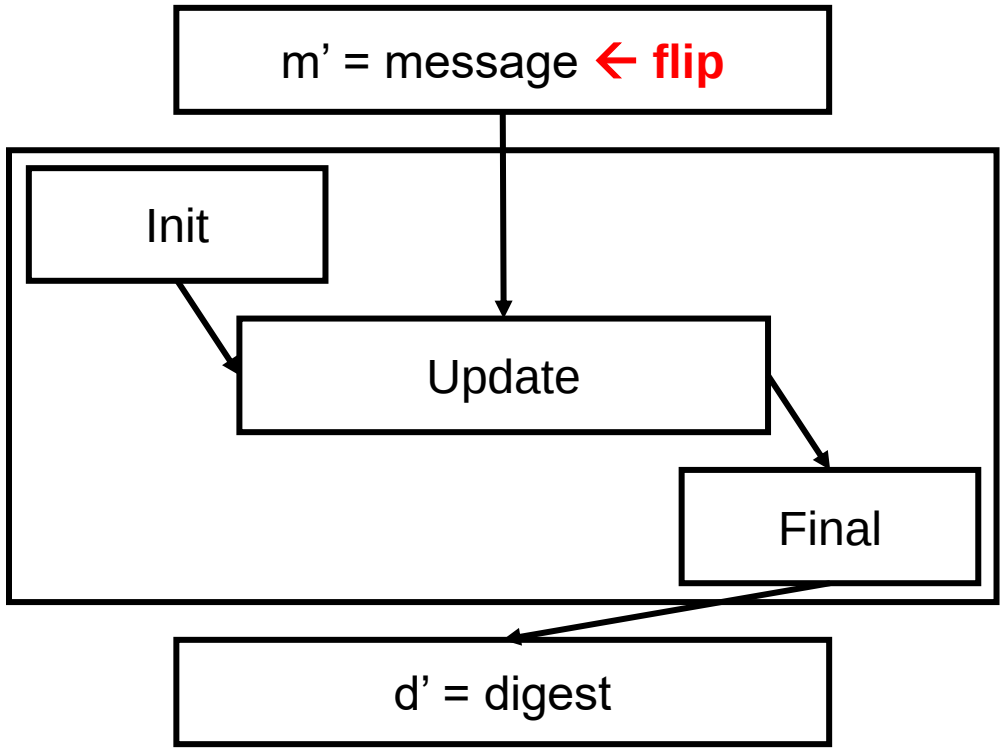
- 기존 테스트 방법은 높은 신뢰도를 가짐
  - 하지만 **알고리즘 내부의 세세한 에러를 파악하기는 어려움**

- Metamorphic Test는 작은 오류를 잡아내는 테스트
  - **알고리즘 동작 자체를 수정**하여 테스트를 진행

Bit-Contribution Test

- 입력 값의 1비트를 반전시켜 동작을 검사
  - 입력 값 1바이트당 실험 횟수는 8회 (e.g. 64바이트 입력 → 512회 실험)
  - **모든 입력 값의 해시 값은 달라야함**





Bit-Contribution Test

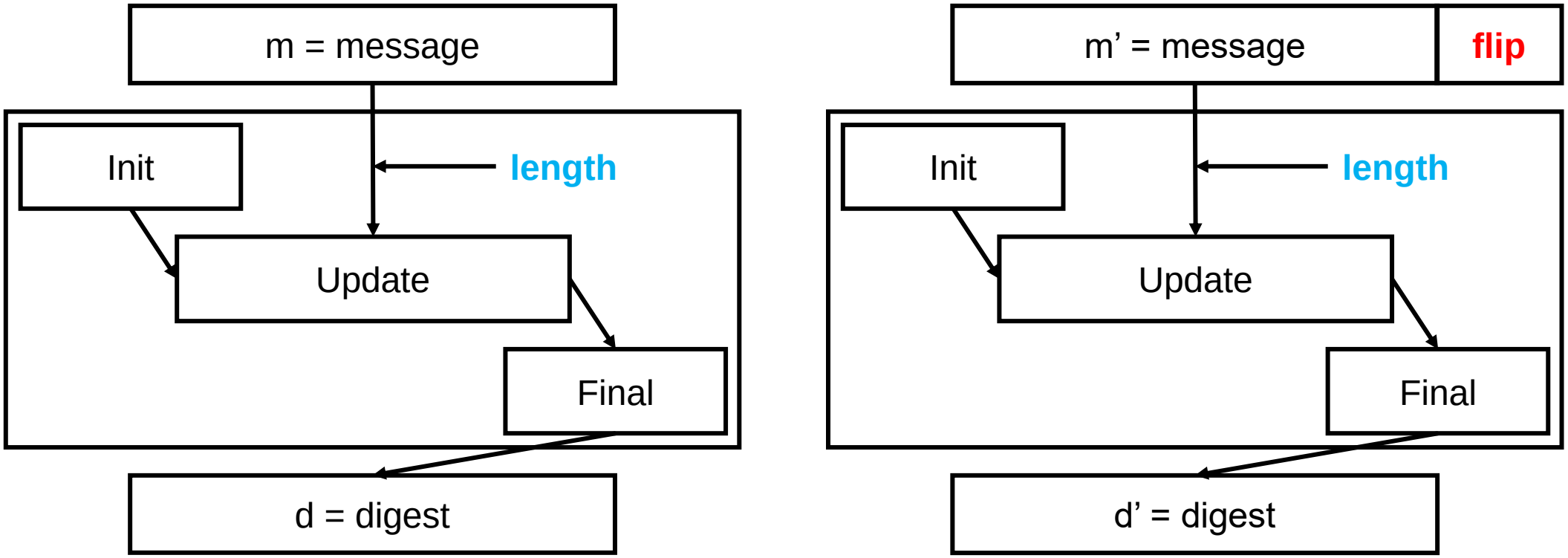
- 입력 값을 1비트 씩 바꿔가며 테스트
- 잘못된 구현이 있다면 해시 충돌 발생 가능
  - 정상적이라면 충돌이 일어나지 않음
- 규모가 크고 번거롭지만,

  코드의 정밀한 구현을 점검하기 좋음

```
abc
Original input: 616263
Original digest: BA7816BF8F01CFEA414140DE5DAE2223B00361A396177A9CB410FF61F20015AD
Test case 1 input: 606263
Test case 1 digest: 89F900390E14D37C405C75244FB086AA35B54C0FB6EC3638C1C21451D4743D11
Test case 2 input: 636263
Test case 2 digest: F1454F676CEB25587D73DEC3E5F5E5BBA4CB8F075D9478F87E66AE9F11068E2D
Test case 3 input: 656263
Test case 3 digest: 05011BA86CF326806EDA4AA8BD9C60BB5609B2BBCB65E1B8E8F72E576CA62DCE
Test case 4 input: 696263
Test case 4 digest: 3263C2FA090392FD141E13070EDCDFE7617A1C3D91648DFD912A4B6A541A8613
Test case 5 input: 716263
Test case 5 digest: 84326588F21E1CACB54C2E24AC2F980CABBC87DE1FED0D5DFC85329E35D1703F
Test case 6 input: 416263
Test case 6 digest: 06D90109C8CCE34EC0C776950465421E176F08B831A938B3C6E76CB7BEE8790B
Test case 7 input: 216263
Test case 7 digest: AC0CED2B1ED66ECCB61915079BC3A82C531CEDE5F750DA669BD9B7E284D83967
Test case 8 input: E16263
Test case 8 digest: C1A192D2F5C898470657C592A56EFB5919A5EA9AC1DC9308ACDFD77990B588CD
Test case 9 input: 616363
Test case 9 digest: 414322309DB5C06D090A2E922CCC3E00708C993B9B96405DE127B7FD8DA2DD21
Test case 10 input: 616063
Test case 10 digest: 14923D06FA1D26943A690E61A212F0A3429A06E274781E82147CC568F8A4533A
Test case 11 input: 616663
Test case 11 digest: F697AAEAA602B1FF3DA09052AF6F7E5193D1D9772D1C7CEAD9EE166256EC5125
Test case 12 input: 616A63
Test case 12 digest: 97782D3EED4BED217C46893D4D73D011A9A68154EC8C83387E728AD451EAEAE2
Test case 13 input: 617263
Test case 13 digest: 404FCFB394D23199F6D95F1F36BD2BEB6DF8564F993F44517F6015FCD16101A9
Test case 14 input: 614263
Test case 14 digest: 516DD854EC42B5B992888CFA87AE16E260864F5E051E045CD7D7C0B45EACBEB2
Test case 15 input: 612263
Test case 15 digest: A4DA799FDFEE19A00C3C5A1E565A4C6576F50AB8BE4893D988DB8BC23C3669B7
Test case 16 input: 61E263
Test case 16 digest: 92EB2D8A6DDAE47AF82449DC0EFDAD64ACC6C6880F5DD9961178E817F9058ECB
Test case 17 input: 616262
Test case 17 digest: 715EDF8BA8729420CD4D1CE85ED61954A9F531F8C548DF728C407EFFE839296D
Test case 18 input: 616261
Test case 18 digest: E124ADCCE1FB2F88E1EA799C3D0820845ED343E6C739E54131FCB3A56E4BC1BD
Test case 19 input: 616267
Test case 19 digest: FBB43C052ACF1843DDACE6CDF93F727A96BD8DD30A70BA93BA9A339FEB4183E3
Test case 20 input: 61626B
Test case 20 digest: A4064CD0F0B5D4A3B025A148FF8152208DF2276871BA294BA1845E15CD10C701
Test case 21 input: 616273
Test case 21 digest: 78DA4A596A88BC5114F071BA590793BF3B37329D761230F33129983A747F414E
```

Bit-Exclusion Test

- 입력 값에 추가적인 임의의 값을 추가
  - 하지만 함수 가동시에 **길이 옵션은 정상 길이**를 사용
  - 임의의 값은 입력되지 않기 때문에 **동일 해시가 출력**되어야 함



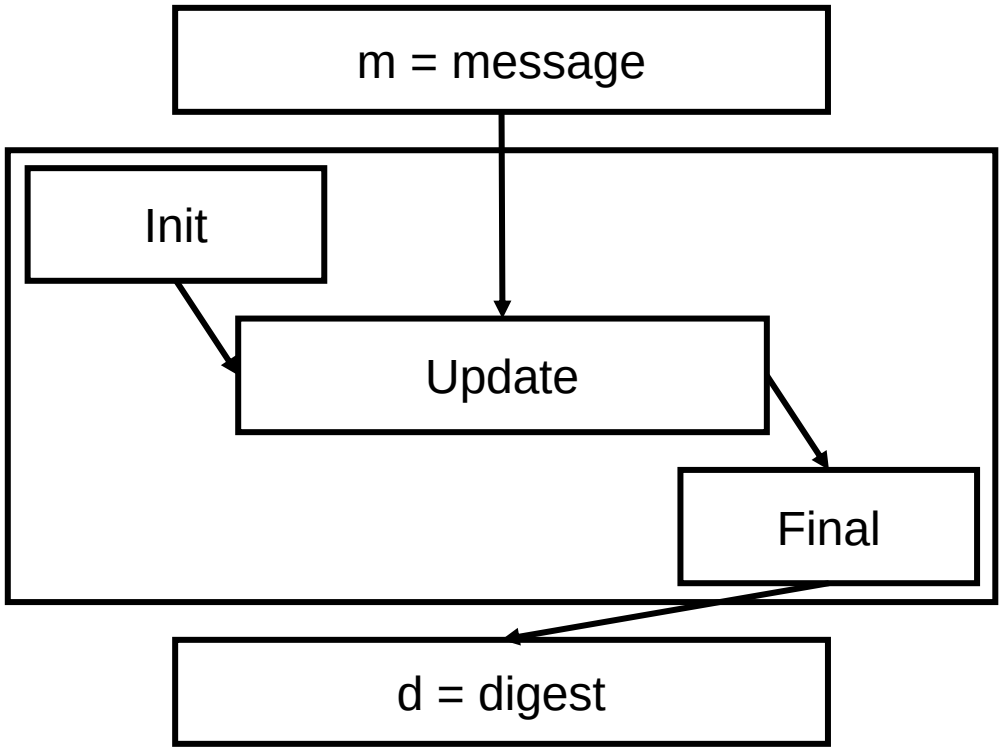
Bit-Exclusion Test

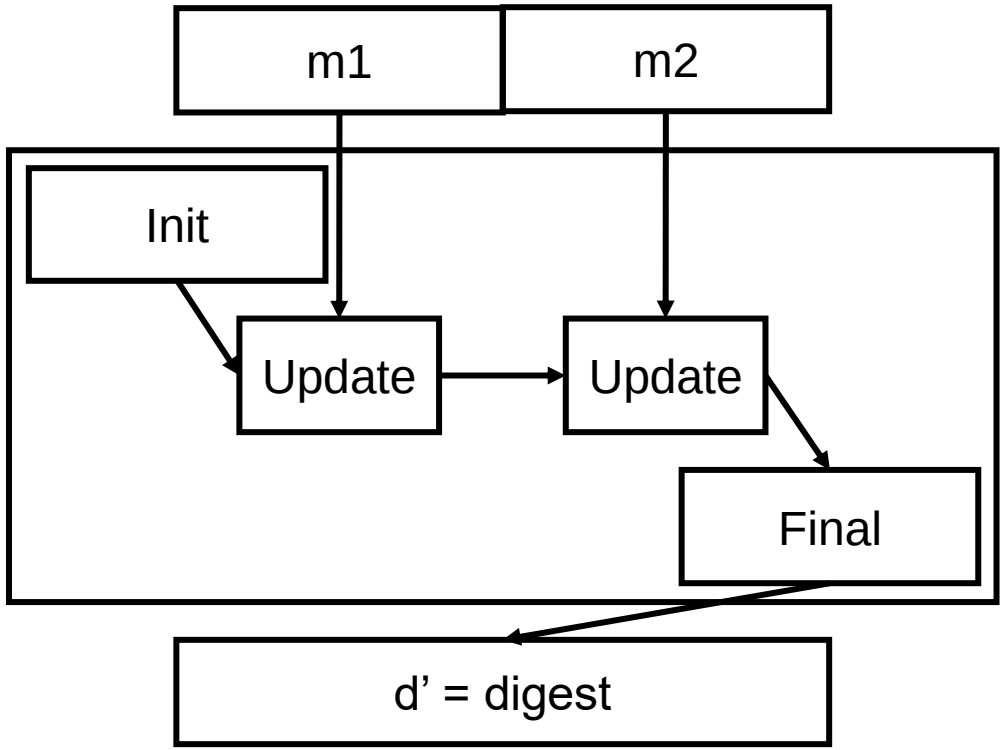
- 인위적인 추가 입력 값을 확인 가능
  - 실제 함수 가동 시에는 메시지 길이 매개변수로 인해 무시되는 부분
- **메시지 길이 관련 체크**가 이루어지는지 확인 가능
  - 해당 부분이 미흡하다면 본 테스트를 통과할 수 없음

```
abc
Original input:         616263
Original digest:        3A985DA74FE225B2045C172D6BD390BD855F086E3E9D525B46BFE24511431532
Test input:             61626361626364
Test digest:            3A985DA74FE225B2045C172D6BD390BD855F086E3E9D525B46BFE24511431532
```

Update Test

- 입력 메시지를 인위적으로 분할하여 갱신 함수를 여러 번 호출
  - 블록암호의 경우, 암호 생성 과정을 호출
- 결과 값 생성 전에는 구조체에 값이 누적될 수 있어야함
  - 따라서 **결과 값은 서로 동일**





Update Test

- 메시지 블록마다 길이를 다르게 동작
  - 하지만 **출력 값은 같은 것을 확인** 가능

```
abcdefghijklmnop
Original input:          61626364656667686 96A6B6C6D6E6F70
Original digest:         C3FAD9C0CC983F7E2D1348BD3EFC56B26363A544FCFF58F728255B8E1EC82A42
Length of each pieces: 11,       2,       1,       2,       Total length: 16
Test input 1:            61626364656667686 96A6B
Test input 2:            6C6D
Test input 3:            6E
Test input 4:            6F70
Test digest:             C3FAD9C0CC983F7E2D1348BD3EFC56B26363A544FCFF58F728255B8E1EC82A42
abcdefghijklmnop
Original input:          61626364656667686 96A6B6C6D6E6F70
Original digest:         C3FAD9C0CC983F7E2D1348BD3EFC56B26363A544FCFF58F728255B8E1EC82A42
Length of each pieces: 5,        1,       4,       6,       Total length: 16
Test input 1:            6162636465
Test input 2:            66
Test input 3:            6768696A
Test input 4:            6B6C6D6E6F70
Test digest:             C3FAD9C0CC983F7E2D1348BD3EFC56B26363A544FCFF58F728255B8E1EC82A42
abcdefghijklmnop
Original input:          61626364656667686 96A6B6C6D6E6F70
Original digest:         C3FAD9C0CC983F7E2D1348BD3EFC56B26363A544FCFF58F728255B8E1EC82A42
Length of each pieces: 1,        2,       3,       10,      Total length: 16
Test input 1:            61
Test input 2:            6263
Test input 3:            646566
Test input 4:            6768696A6B6C6D6E6F70
Test digest:             C3FAD9C0CC983F7E2D1348BD3EFC56B26363A544FCFF58F728255B8E1EC82A42
```

결론

- Metamorphic Test는 알고리즘 내부 동작을 수정하여 테스트
  - **실제로 내부 동작을 수정하지는 않음**
  - 암호 라이브러리 호출을 다르게 하여 테스트 진행
- 세밀한 동작의 오류를 검출할 수 있음
  - 테스트 종류에 따라 결과 값이 서로 일치하지 않는 경우에도 통과할 수 있음
- 암호 구현의 적합성을 검사하기 위해 본 테스트를 진행하는 것이 좋음
  - **세부적인 오류를 점검**할 수 있는 방법

Q & A