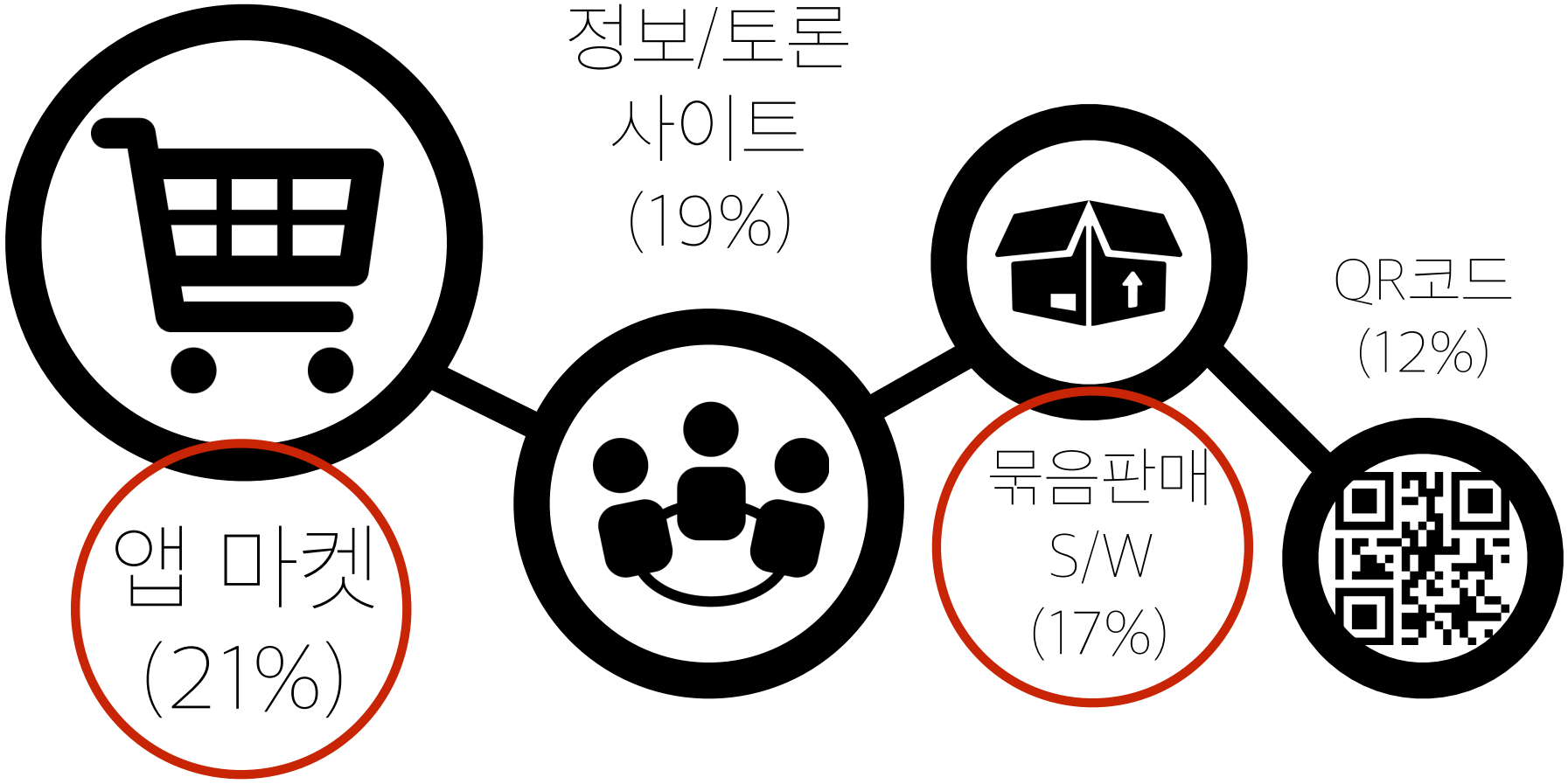
시사로
쉽게 이해해보는
보안 이야기

- 스마트폰 편 -

우리 스마트폰 안에는...

이동전화 바이러스 전파경로

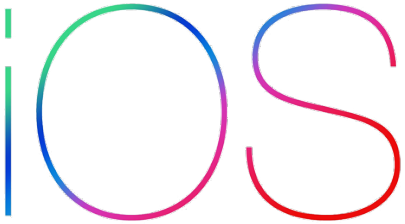


바이러스 전파는 주로 어플리케이션 설치를 통해 이루어진다.

[中 3분기 정보보안 보고 ③] 이동전화 바이러스 전파경로
http://www.boannews.com/media/view.asp?idx=48459&kind=3

인증되지 않은 앱을 설치하는 법

환경설정 -> 보안 탭
-> **'알 수 없는 출처'에 체크**



휴대전화 **루팅(Jailbreak)**
-> Cydia를 통한 설치

iOS는 정식 앱스토어 이외의 방법으로
어플리케이션 설치가 금지되어 있다.

iOS 보안취약점: XcodeGhost

악성 엑스코드 버전은 어떤 앱이든
컴파일 할 수 있는 기능이 추가된다.

해로운 기능의 앱이
정식 등록되는 것이다!

이로써 iOS 생태계의
맬웨어 탐지 시스템을 우회,
정식 앱스토어에 등록된다.

"확대되는 엑스코드고스트 사태" 파이어아이, 감염된 iOS 앱 4,000여개 발견, http://www.itworld.co.kr/news/95727

iOS 보안취약점: XcodeGhost

Top 25 Apps Compromised by XcodeGhost Malware

- **WeChat**
- DiDi Taxi
- 58 Classified – Job, Used Cars, Rent
- Gaode Map – Driving and Public Transportation
- Railroad 12306
- Flush
- **China Unicom Customer Service (Official Version)***
- **CarrotFantasy 2: Daily Battle***
- Miraculous Warmth
- Call Me MT 2 – Multi-server version
- **Angry Birds 2 - Yifeng Li's Favorite***
- **Baidu Music - Music Player with Downloads, Ringtones, Music Videos, Radio & Karaoke**
- DuoDuo Ringtone
- NetEase Music – An Essential for Radio and Song Download
- **Foreign Harbor - The Hottest Platform for Oversea Shopping***
- Battle of Freedom (The MOBA mobile game)
- **One Piece - Embark (Officially Authorized)***
- Let's Cook – Receipes
- **Heroes of Order & Chaos - Multiplayer Online Game***
- **Dark Dawn - Under the Icing City (the first mobile game sponsored by Fan BingBing)***
- **I Like Being With You***
- Himalaya FM (Audio Book Community)
- **CarrotFantasy***
- Flush HD
- Encounter – Local Chatting Tool

Apple Lists Top 25 Apps Compromised by XcodeGhost Malware, http://www.macrumors.com/2015/09/24/xcodeghost-top-25-apps-apple-list/

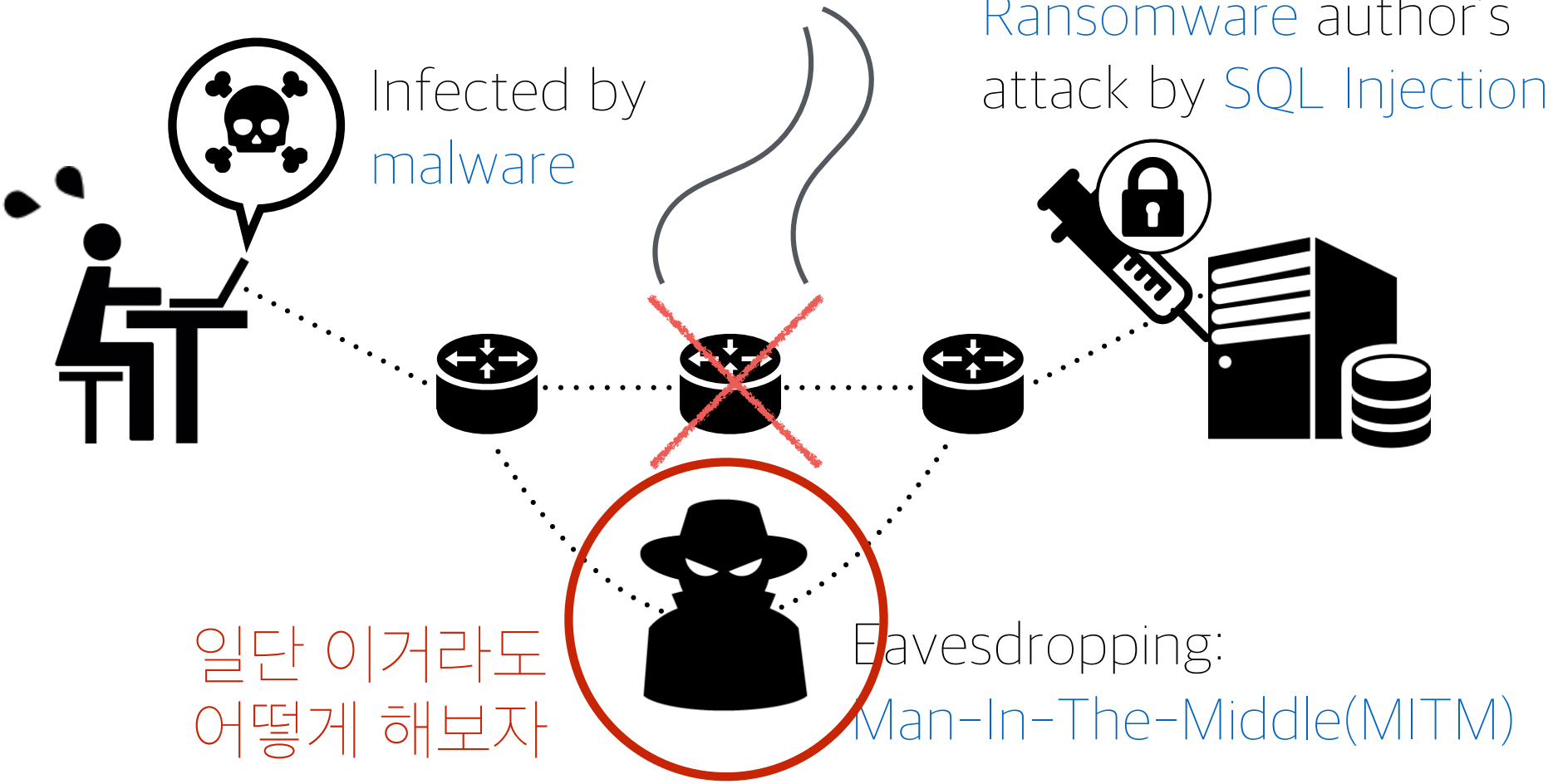
어떤 이유에서건
우리 개인정보는 이미 공공재

개인정보가
데이터베이스화
되어가고 있다

한국 주민등록번호를 입력하면 진위를 알려주는 중국 사이트(왼쪽). '한국신분증' 코너의 검색창에 실제 인물의 주민번호를 입력하자 중국어로 '합법적인 번호입니다'라는 메시지(녹색 글씨)와 함께 성별·나이·생년월일 등의 정보가 나타났다. 오른쪽은 한 중국 네티즌이 인터넷에서 검색해 블로그에 올린 한국인의 실제 주민등록증 사진.

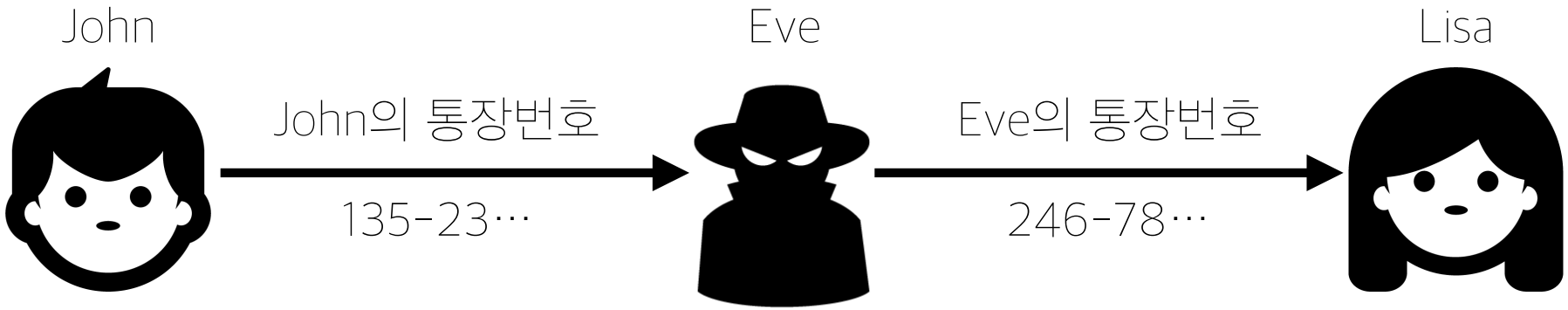
[기획] 한국인 개인정보 DB화해 서비스하는 중국 사이트… 주민번호 입력하자 '사용 가능' 문구, http://news.kmib.co.kr/article/view.asp?arcid=0008140779&code=11131100

안전한 곳은 없다


Infected by
malware
Ransomware author's
attack by SQL Injection
일단 이거라도
어떻게 해보자
Eavesdropping:
Man-In-The-Middle(MITM)

상황을 조금이나마 해결해보자

중간자 공격(man in the middle attack, MITM)은 네트워크 통신을 조작하여 **통신 내용을 도청하거나 조작**하는 공격 기법이다. 중간자 공격은 통신을 연결하는 두 사람 사이에 중간자가 침입하여, **두 사람은 상대방에게 연결했다고 생각**하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 **전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달**한다.

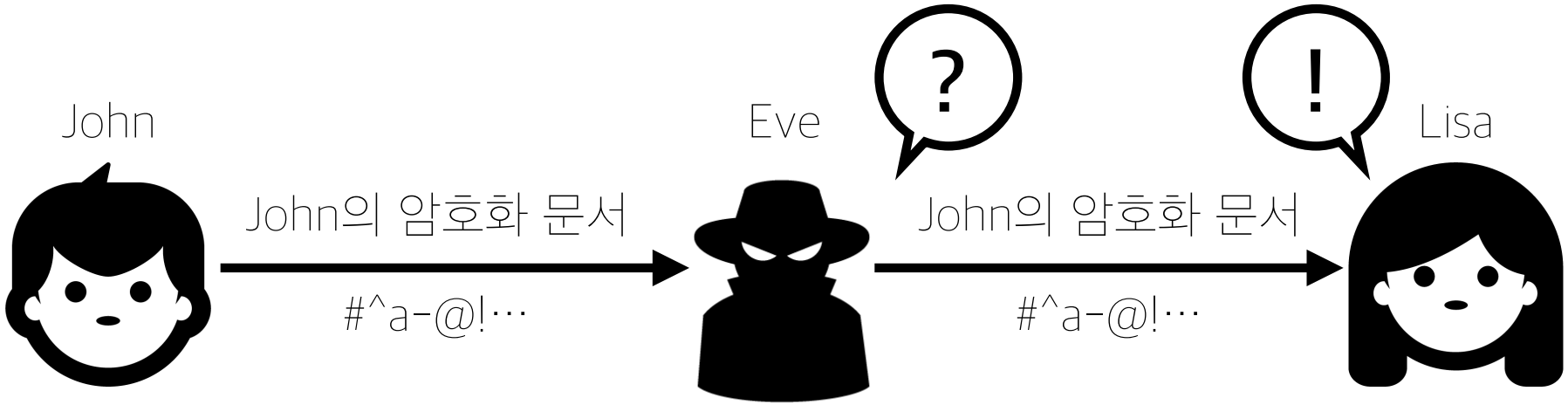


중간자공격, https://ko.wikipedia.org/wiki/%EC%A4%91%EA%B0%84%EC%9E%90_%EA%B3%B5%EA%B2%A9

상황을 조금이나마 해결해보자

‘Eve’가 내용을 모르게 해야 한다 !

공개 키 암호방식이 가장 만만하다



상황을 조금이나마 해결해보자

공개 키 암호 방식

공개 키는 누구나 소유할 수 있다.
공개 키를 이용하여 문서를 암호화하게 되면,
비밀 키를 이용해야만 문서를 해독할 수 있게 된다.

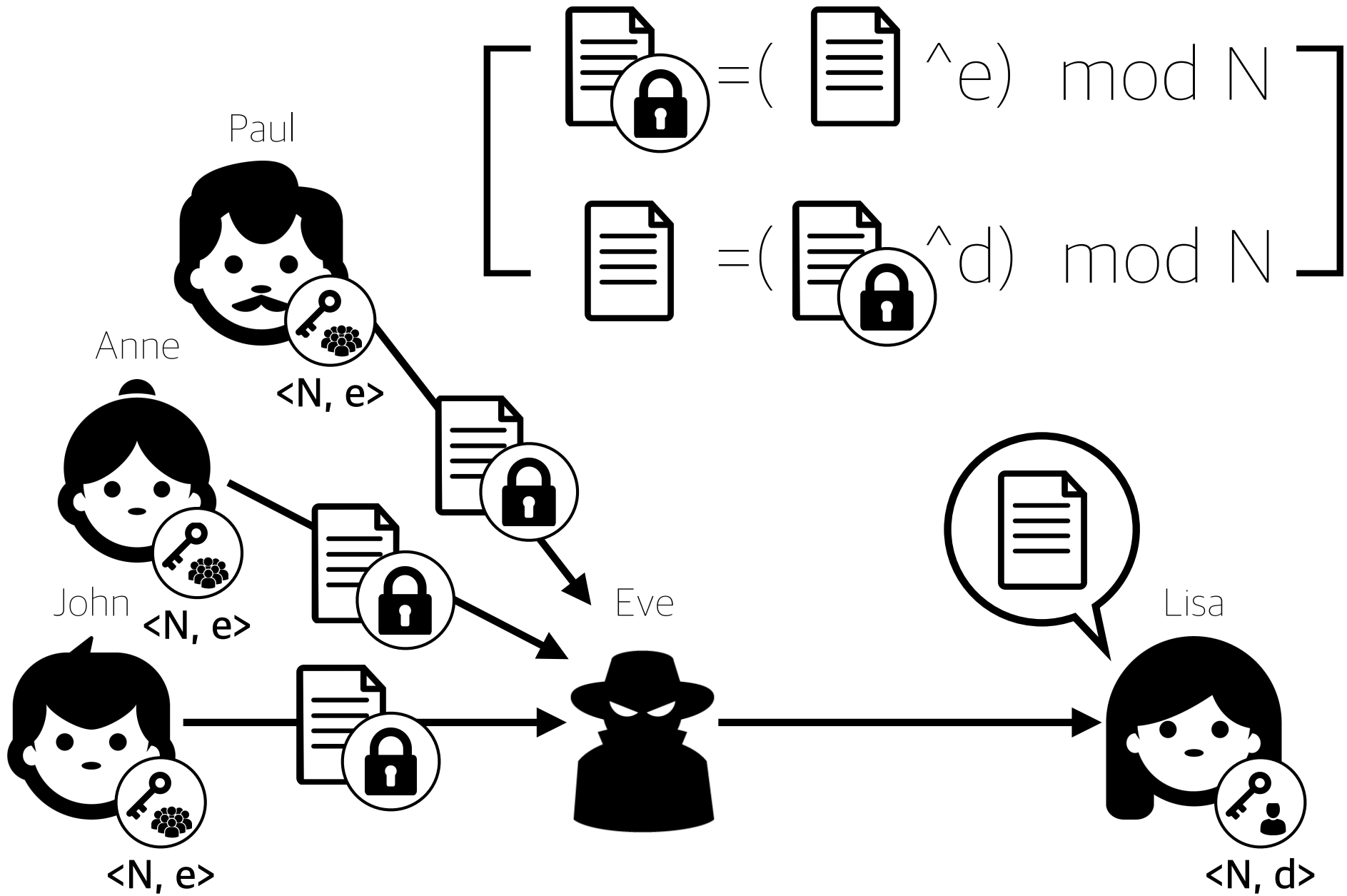
공개 키 암호 방식, https://ko.wikipedia.org/wiki/%EA%B3%B5%EA%B0%9C_%ED%82%A4_%EC%95%94%ED%98%B8_%EB%B0%A9%EC%8B%9D

상황을 조금이나마 해결해보자

RSA 암호

소인수 분해의 난해함에 기반하여,
공개 키 만을 가지고는 개인 키를 쉽게
짐작할 수 없도록 디자인되어 있다.

RSA 암호, https://ko.wikipedia.org/wiki/RSA_%EC%95%94%ED%98%B8


=(^e) mod N
=(^d) mod N
Paul
<N, e>
Anne
<N, e>
John
<N, e>
Eve
Lisa
<N, d>

1. 키 생성에 사용된 소수 혹은 비밀 키 등이
   도난 당하지 않는 이상, 문서가 해독될
   가능성은 매우 희박하다.
2. 여기서 John의 비밀 키로 문서를 암호화 한다면,
   오직 John의 공개 키로만 문서가 해독된다.
   이는 문서의 저자가 John임을 증명한다.
3. 따라서 RSA는 지금도 전자서명 알고리즘으로
   주로 사용되고 있다.