Cryptography presentation

As part of the lecture *Kryptographie und Sicherheit in Verteilten Systemen*

L. Herich A. Plötze
Freie Universität Berlin

Berlin, 2015

Outline

Lecture content

Encryption schemes

Eavesdropping (EAV)
Known-plaintext attack (KPA)
Chosen-plaintext attack (CPA)
Chosen-ciphertext attack (CCA)

Signature schemes

Adaptive-chosen-message attack (ACMA)

Git repository with topics of the lecture

- shift cipher
- vigenere cipher

- modern
  - symmetric (secret-key)
    - encryption schemes
      - stream cipher
      - block cipher
        - substitution-permutation-networks
          - S-boxes
          - P-Boxes
        - feistel-networks
        - modes of operation
          - electronic codebook mode (ECB)

Figure : Git repository with the summarized topics of the lecture

Fork it on github.com

- `https://github.com/lherich/cryptography`
- `git@github.com:lherich/cryptography.git`

Attacks on encryption schemes

The adversarial indistinguishability experiment $PrivK^{EAV}_{A,\Pi}$

$\Pi = (Gen, Enc, Dec)$ is any private-key encryption scheme, A is the adversary, M message space, n is the security paramter

1. $(m_0, m_1) \in M \leftarrow A$
2. $k \xleftarrow{\$} Gen(1^n)$
3. $b \xleftarrow{\$} \{0, 1\}$
4. $c \leftarrow Enc_k(m_b)$
5. c is given to A
6. $b' \leftarrow A$
7. $if (b = b')\ output\ 1$
   $else\ output\ 0$

indistinguishable encryptions in the presence of an eavesdropper: if for all probabilistic polynomial-time adversaries A:

$$\left| \frac{1}{2} - Pr[PrivK^{EAV}_{A,\Pi}(n) = 1] \right| \leq negl(n)$$

Eavesdropping (EAV)

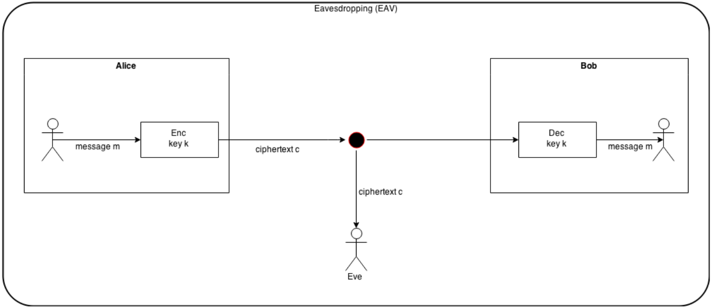

Figure : Eavesdropping (EAV)

IND-EAV can be constructed by a PRG[1]

[1] Katz and Lindell: Introduction to Modern Cryptography, 2007 p. 73

Known-plaintext attack (KPA)

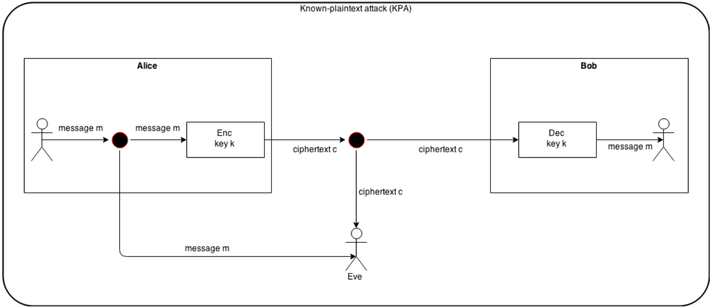

Figure : Known-plaintext attack (KPA)

Chosen-plaintext attack (CPA)

The CPA indistinguishability experiment $PrivK^{CPA}_{A,\Pi}(n)$:

$\Pi = (Gen, Enc, Dec)$ is any private-key encryption scheme, A is the adversary, n is the security paramter.

1. $k \xleftarrow{\$} Gen(1^n)$
2. $(m_0, m_1) \leftarrow A^{Enc_k(.)}(1^n)$
3. $b \xleftarrow{\$} \{0, 1\}$
4. $c \leftarrow Enc_k(m_b)$
5. c is given to A
6. $b' \leftarrow A^{Enc_k(.)}(c)$
7. $if (b = b')\ output\ 1$
   $else\ output\ 0$

CPA-secure: if for all probabilistic polynomial-time adversaries A:

$$\left| \frac{1}{2} - Pr[PrivK^{CPA}_{A,\Pi}(n) = 1] \right| \leq negl(n)$$

Chosen-plaintext attack (CPA)

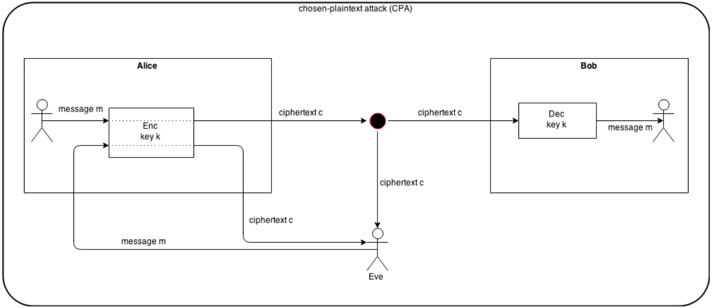

Figure : Chosen-plaintext attack (CPA)

IND-CPA can be constructed by a PRF[2]

[2] Katz and Lindell: Introduction to Modern Cryptography, 2007 p. 89

Chosen-ciphertext attack (CCA)

The CCA indistinguishability experiment $PrivK^{CCA}_{A,\Pi}(n)$

$\Pi = (Gen, Enc, Dec)$ is any private-key encryption scheme
A is the adversary
n is the security paramter

1. $k \xleftarrow{\$} Gen(1^n)$
2. $(m_0, m_1) \leftarrow A^{Enc_k(.),Dec_k(.)}(ask, 1^n)$
3. $b \xleftarrow{\$} \{0, 1\}$
4. $c \leftarrow Enc_k(m_b)$
5. $b' \leftarrow A^{Enc_k(.),Dec_k(.)}(guess, c)$
6. $if (b = b')\ output\ 1$
   $else\ output\ 0$

CCA-secure: if for all probabilistic polynomial-time adversaries A:
$\left|\frac{1}{2} - Pr[PrivK^{CCA}_{A,\Pi}(n) = 1]\right| \leq negl(n)$

Chosen-ciphertext attack (CCA)

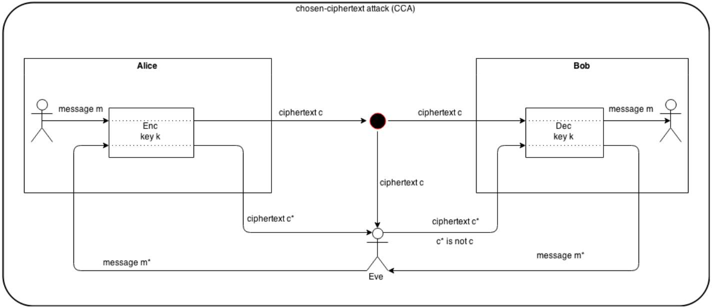

Figure : Chosen-ciphertext attack (CCA)

CBC, OFB and CTR-Mode are not CCA2-secure encryption schemes for every F (see assignment 6).
CCA1/CCA2 can be constructed from a CPA-secure encryption scheme and an ACMA secure MAC (PRF)[3].

[3] Katz and Lindell: Introduction to Modern Cryptography, 2007 p. 89

Attacks on MAC/signature schemes

Adaptive-chosen-message attack (ACMA)

The message authentication experiment MAC-forge$_{A,\Pi}(n)$

1. $k \xleftarrow{\$} \{0,1\}^n$
2. $(m,t) \leftarrow A^{MAC_k(.)}(1^n)$
3. $if\,(m \notin Q \text{ } and \text{ } Vrfy_K(m,t) = 1) \text{ } output \text{ } 1$
   $otherwise \text{ } output \text{ } 0$

A MAC-scheme Π is secure against adaptive-chosen-message-attacks, if for all probabilistic polynomial-time adversaries A, there exists a negligible function negl, such that:
$Pr[\text{MAC-forge}_{A,\Pi}(n) = 1] \leq negl(n)$

Adaptive-chosen-message attack (ACMA)

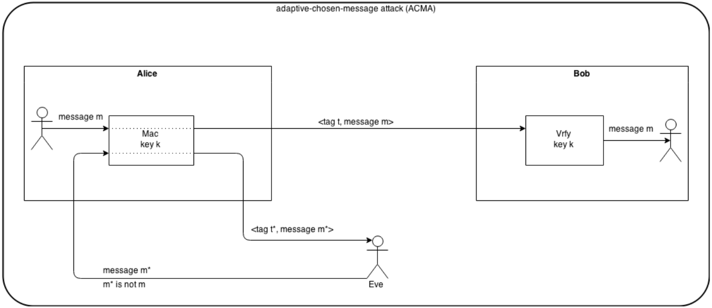

Figure : Adaptive-chosen-message attack (ACMA)

Any annotations or questions?