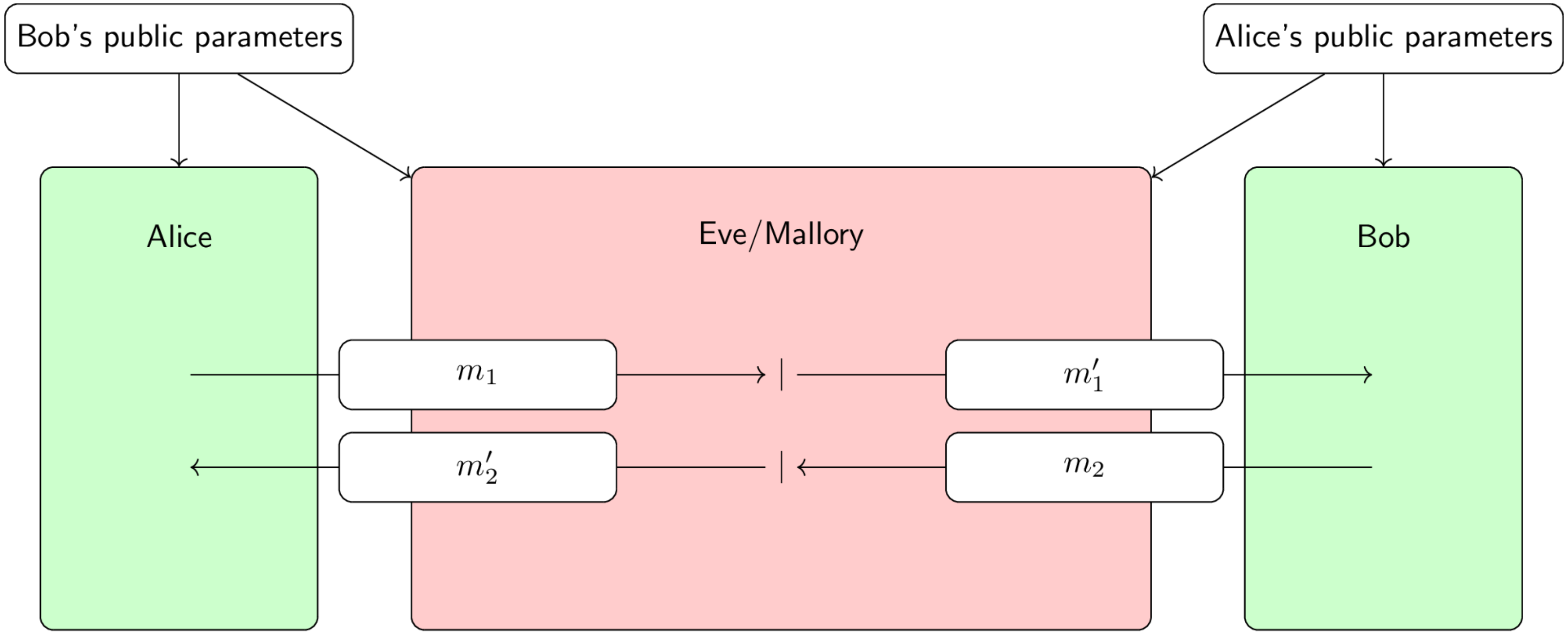
esse

Advanced Security for Systems Engineering – VO 10: Applied Cryptography

Clemens Hlauschek
Christian Brem

Threat Model: Passive vs Active

Threat Model



Passive: $m_i = m'_i$

Adversaries Capabilities

- Depend on exact model
  - Passive: eavesdropping
  - Active: tampering with, blocking, delaying, reordering messages
  - Advanced active: corrupting some peers, etc (multiparty setting)

- Mostly: Probabilistic Polynomial Time (PPT) adversary
- If unsure, use most conservative model/most powerful adversary
- Always assume active advesary in a networking setting

Important Notions

- Ciphertext Indistinguishablility
- Semantic Security
- Chosen Plaintext Attack
- Chosen Ciphertext Attack
- IND-CPA, IND-CCA, IND-CCA2

Game-Based Security Definintions

Blackboard

Threat Model: Limitations

Brainstorming Attacks

Common Attacks against Crypto

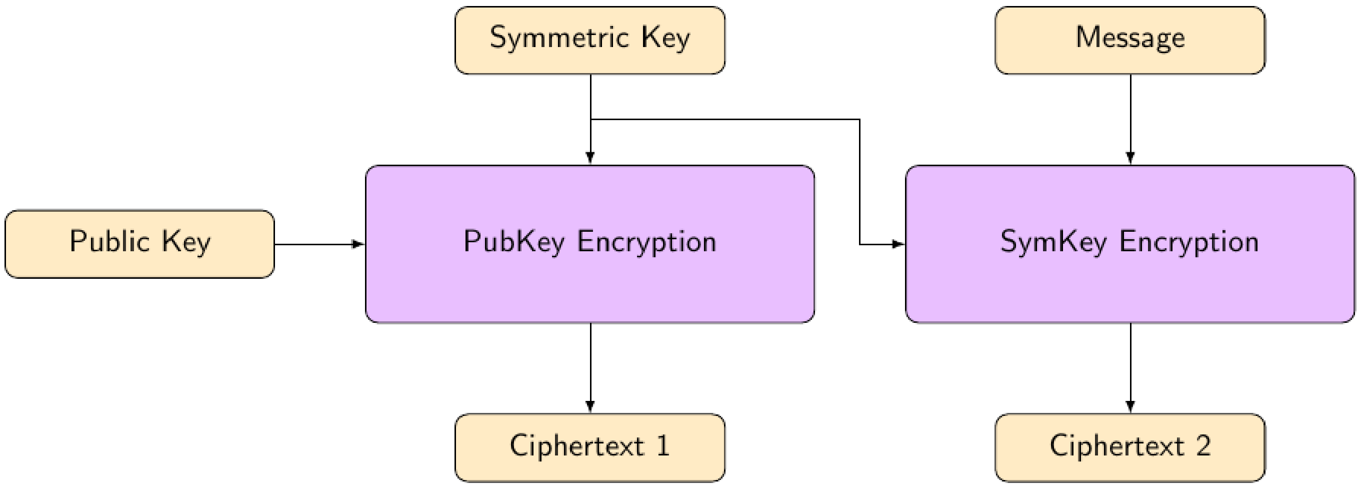
- Use of wrong protocol, insufficient security guarantees
- Protocol errors
- Implementation errors
- Side-channel attacks, Fault injection
- Statistical attacks, attacks on traffic patterns
- Compromise infrastructure, trust anchors

Which are Out-of-Model attacks?

Encryption Schemes

Encryption Algorithms: Keywords

- Symmetric, Secret-key: $m = D(k, E(k, m))$
  - 3DES, AES, (X)Salsa20, ChaCha
  - Fast, but Key Distribution problem
- Asymmetric, Public-key: $m = D(sk, E(pk, m))$
  - RSA, ElGamal, Elliptic Curves
- Hybrid:



Prove-Driven Design

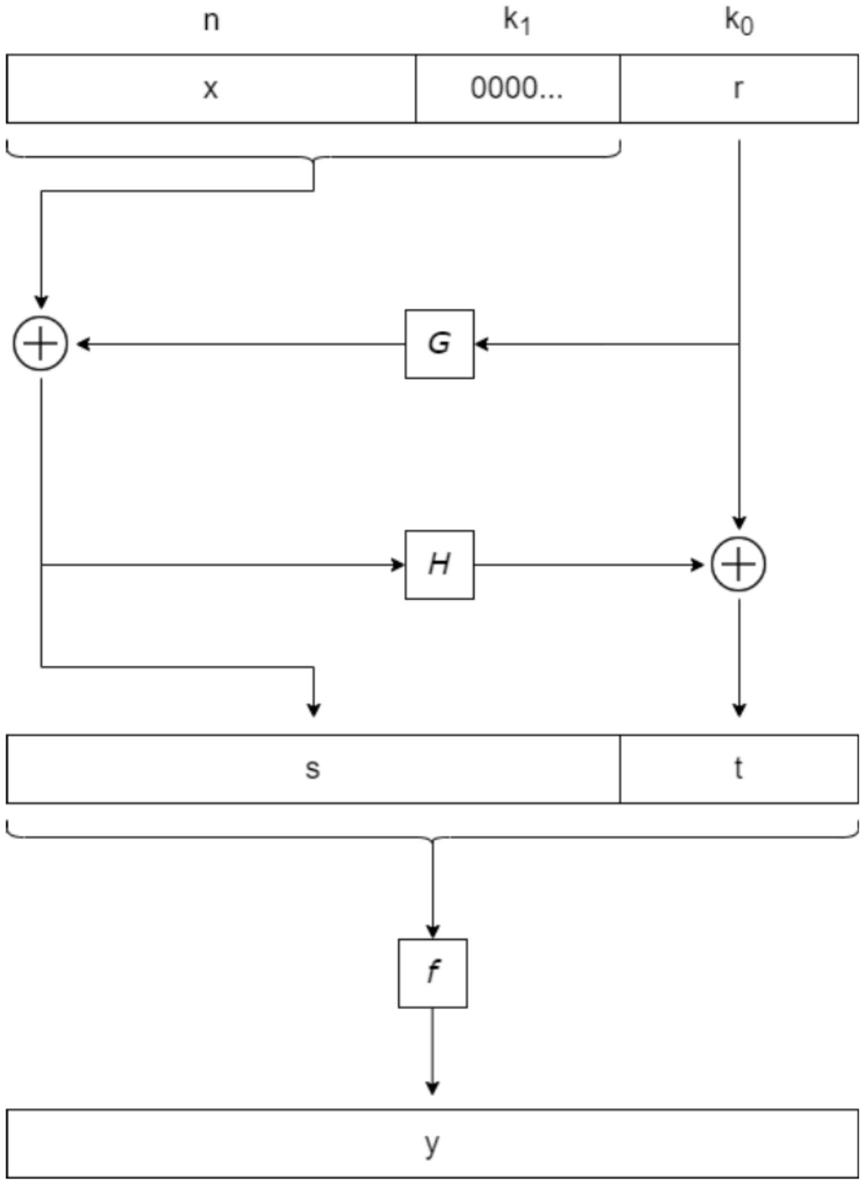
From Oneway Function/PRP to Secure Cryptographic Scheme

1. Oneway function (with trapdoor)/pseudorandom permutation (PRP)
2. Hardness assumptions
3. Threat model and goals (IND-CCA, IND-CPA)
4. Secure cryptographic scheme with reduction to hardness assumption

RSA Cryptosystem

- **Assumption:**
  - Hardness related to Integer Factorization problem
- **Basic Primitive:**
  - $N = p \cdot q$ with $p, q \in \mathbb{P}$
  - Operations are computed $\mod N$
  - $sk : d \quad pk : e$ with $e \cdot d = 1 \mod \phi(N)$
  - $E : m^e$
  - $D : m^d$
- **Secure Scheme:**
  - Never use plain (textbook) RSA, use OAEP or at least PKCSv1.5

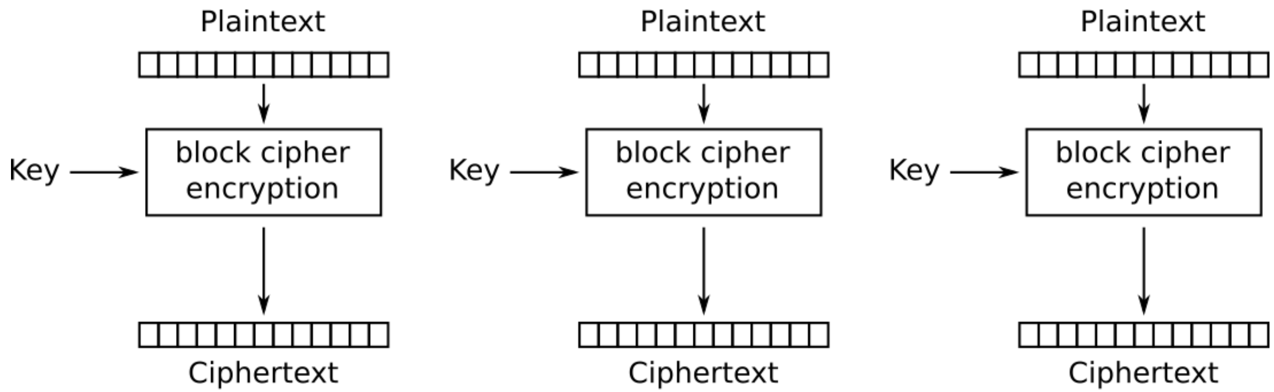
IND-CCA Security for RSA: OAEP



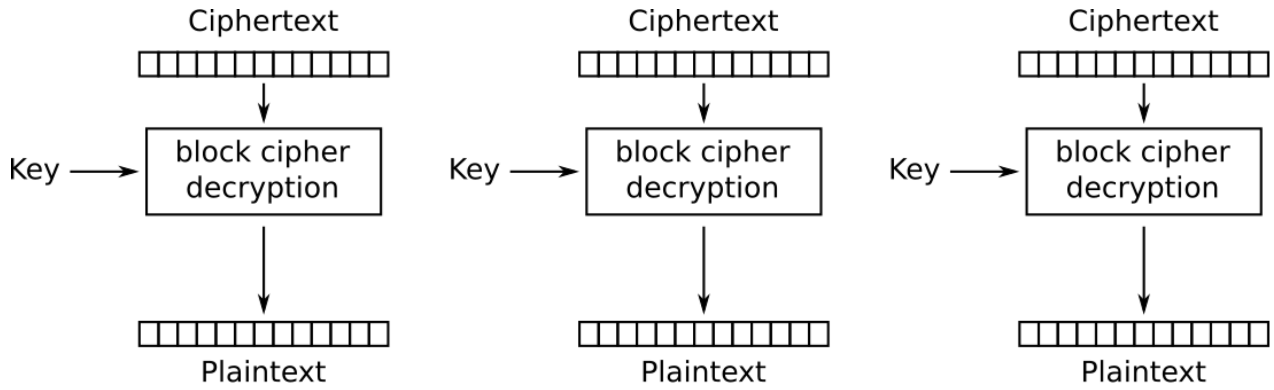
ElGamal/Cramer-Shoup Cryptosystem

- **Assumption:**
  - Hardness of Discrete Logarithm, Decisional Diffie-Hellman (DDH)
- **Basic Primitives** (ElGamal)
  - $p \in \mathbb{P}$, g is generator of $\mathbb{Z}_p$
  - Operations are computed $\mod P$
  - $sk : x \quad pk : g^x$ with x uniform random sampled in $\mathbb{Z}_p$
  - $E : (c_0 = g^y, c_1 = pk^y \cdot m)$ with y uniform sampled in $\mathbb{Z}_p$
  - $D : \frac{c_1}{(c_0)^x}$
- **Secure Scheme:**
  - Cramer-Shoup extends Elgamal and is IND-CCA2 secure (DDH)

Electronic Codebook (ECB) Mode



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

ECB Problems

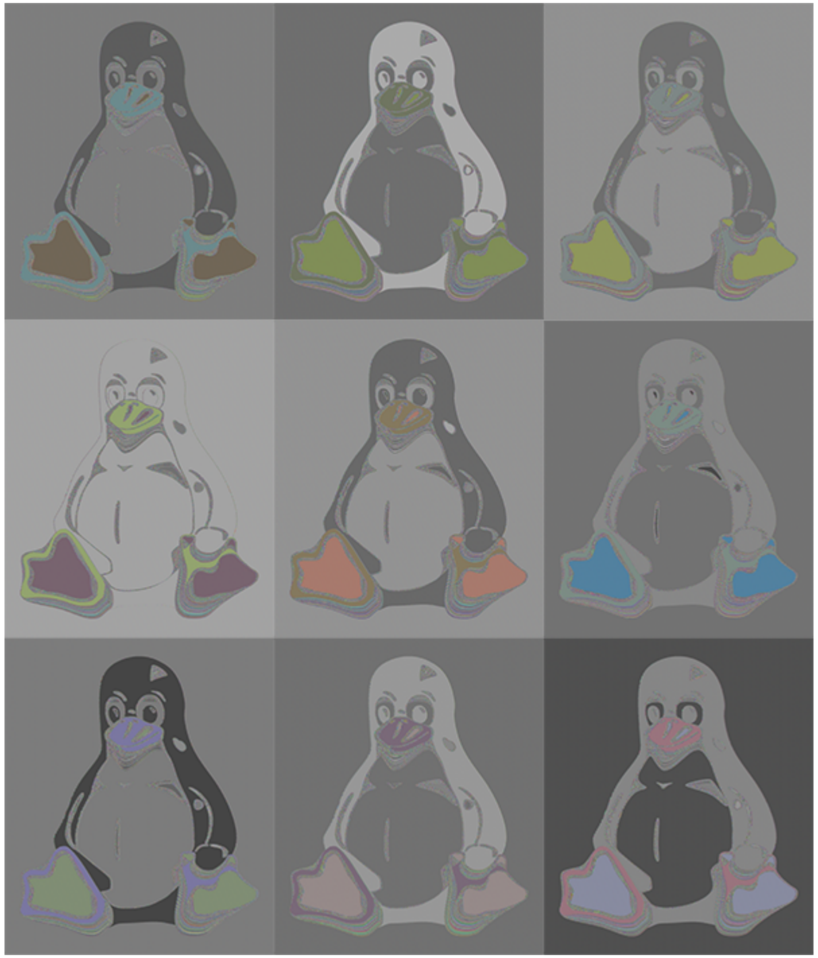
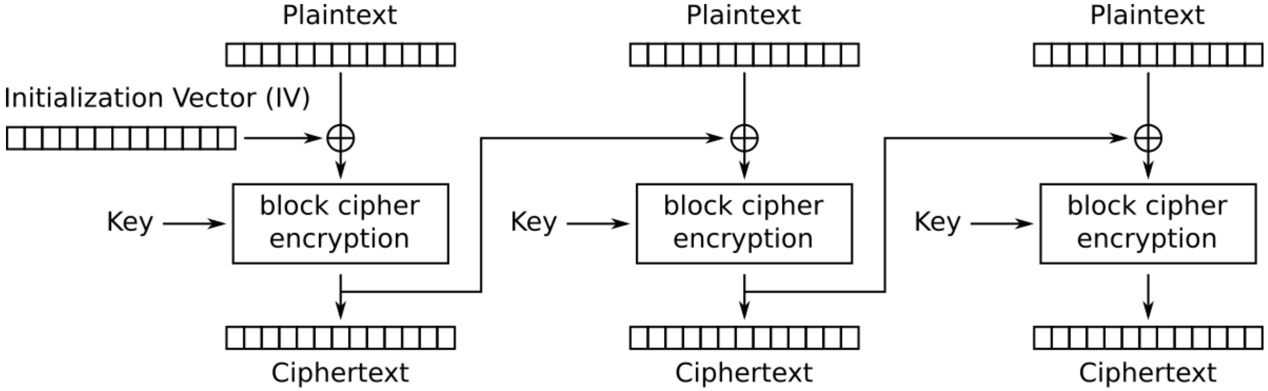
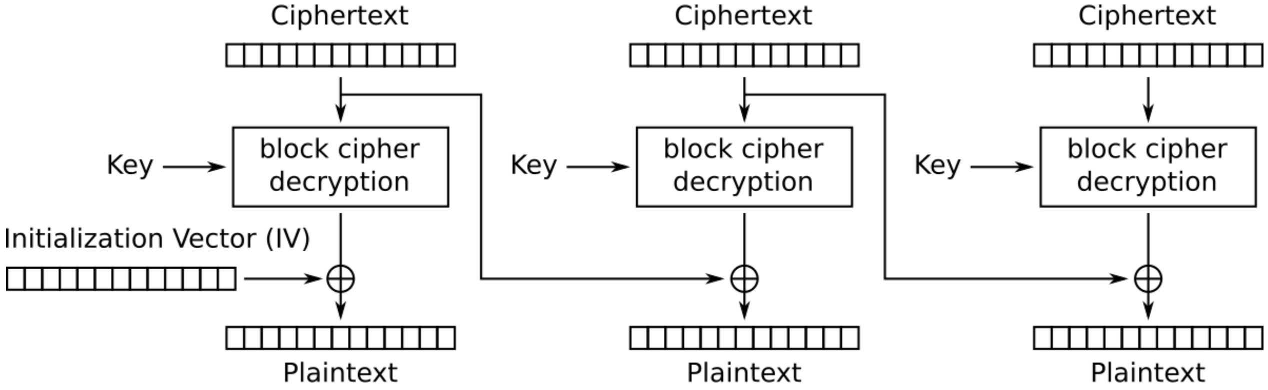


Figure 1: https://blog.filippo.io/the-ecb-penguin/

CBC



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Literature/Links

- Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography, CRC Press, 2014
- Vaudenay: Security Flaws Induced by CBC Padding. Applications to SSL, IPSEC, WTLS. EUROCRYPT'02
- Boeck, et al: Return Of Bleichenbacher's Oracle Threat (ROBOT), Usenix Sec'18
- NaCl Library, `nacl.cr.yp.to`
- Libsodium Library, `libsodium.org`
- [Boneh] Dan Boneh (Stanford): Online Cryptography Class. `http://crypto-class.org`

Thank's for your attention!

https://security.inso.tuwien.ac.at/