Course Summary

Yu Zhang

HIT/CST/NIS

Cryptography, Spring, 2012

Introduction

- Modern cryptography secures information, transactions and computations.
- Kerckhoffs's principle & Open cryptographic design.
- Caesar's, shift, Mono-Alphabetic sub., Vigenère.
- Brute force, letter frequency, Kasiski's, IC.
- Sufficient key space principle.
- Arbitrary adversary principle.
- Rigorously proven security.

Perfect Secrets

- Perfect secrecy = Perfect indistinguishability = Adversarial indistinguishability.
- Perfect secrecy is attainable. The One-Time Pad (Vernam's cipher).
- Shannon's theorem.

Computational Security vs. Info.-theoretical Security

	Computational	**Info.-theoretical**
Adversary	PPT eavesdropping	no limited eavesdropping
Definition	indistinguishable $\frac{1}{2}$ + negl	indistinguishable $\frac{1}{2}$
Assumption	pseudorandom	random
Key	short random str.	long random str.
Construction	XOR pad	XOR pad
Prove	reduction	-

Private-Key Encryption

- Asymptotic approach, proof of reduction, indistinguishable.
- PRG, PRF, PRP, stream cipher, block cipher.
- Security/construction against eavesdropping/CPA.
- EBC, CBC, OFB, CTR.

Block Cipher

- Block cipher is PRP.
- confusion & diffusion, SPN, Feistel network, avalanche effect.
- DES, 3DES, AES.
- reduced round, meet-in-the-middle, differential and linear cryptanalysis.

MAC

- adaptive CMA, replay attack, birthday attack.
- existential unforgeability, collision resistance.
- CBC-MAC, CRHF, Merkle-Damgård transform, NMAC, HMAC.

CCA, AE

- CCA-secure, AE, det. enc., det. CPA-secure, DAE.
- Enc-then-auth, KDF, SIV, wide block cipher, tweakable encryption.
- SIV-CTR, PBKDF, salt, enc. w/o expansion, CTS.

OWF

- OWF implies secure private-key encryption scheme and MAC.
- Secure private-key encryption scheme/MAC implies OWF.

Number Theory, RSA

- Primes, modular arithmetic.
- Miller-Rabin primality testing.
- Factoring, Pollard's $p-1$ and ρ methods.
- e^{th}-root modulo N, RSA.

Public-key Encryption, RSA

- eavesdropper=CPA, CCA/CCA2 in public-key encryptions.
- hybrid argument, multiple encryptions.
- hybrid encryption, "textbook RSA", padded RSA, PKCS.
- small e, common modulus attacks, CCA, faults attack.

DL, CDH/DDH

- cyclic group, discrete log., baby-step/giant-step
- CDH, DDH, DHKE protocol.
- Elgamal encryption, sharing public parameters.

TPD, ROM, and More

- public key encryption from tpd
- random oracle model vs. standard model
- CPA/CCA in ROM, RSA-FDH
- Coldwasser-Micali, Rabin, Paillier (homomorphic with $+$), elliptic curve.

Digital Signature

- Textbook RSA, Hashed RSA, Hash-and-Sign, DSS.
- Lamport's OTS/Stateful/Chain-based/Tree-based/Stateless.
- Certificates, PKI, CA, Web-of-trust, Invalidation.

Cryptographic Protocols

- Man-in-the-middle attack, interlock protocol.
- Shamir three pass protocol.
- Blind signature.
- Secret sharing.
- Commitment scheme, coin flipping.
- Interactive proof, Schnorr protocol, Zero knowledge proofs
- Oblivious transfer, Rabin's, 1-out-of-2.
- Multi-party computation, dining cryptographers problem.
- Quantum cryptography, BB84.

Provable Security

- A proof of security never proves security in an absolute sense, it relates security to an unproven assumption that some computational problem is hard.
- The quality of a security reduction should not be ignored – it matters how tight it is, and how strong the underlying assumption is.
- A security reduction only proves something in a particular model specifying what the adversary has access to and can do.

Crypto Pitfalls

Crypto deceptively simple

- Why does it so often fail?

Important to distinguish various issues:

1. Bad cryptography/implementations/design, etc.
2. Good cryptography can be 'circumvented' by adversaries operating 'outside the model'
3. Even the best cryptography only shifts the weakest point of failure to elsewhere in your system
4. Systems are complex: key management; social engineering; insider attacks

Avoid the first; be aware of 2-4.

Crypto is difficult to get right

- Must be implemented correctly
- Must be integrated from the beginning, not added on "after the fact"
- Need expertise; "a little knowledge can be a dangerous thing"
- Can't be secured by Q/A, only (at best) through penetration testing and dedicated review of the code by security experts

General Recommendation

- Use only standardized algorithms and protocols
- No security through obscurity!
- Use primitives for their intended purpose
- Don't implement your own crypto
- If your system cannot use "off-the-shelf" crypto components, re-think your system
- If you really need something new, have it designed and/or evaluated by an expert
- Don't use the same key for multiple purposes
- Use good random-number generation

Crypto Libraries

- Use existing, high-level crypto libraries: cryptlib, NaCl, Google's Keyczar, Mozilla's NSS, OpenSSL
- Avoid low-level libraries (like JCE, crypto++, GnuPG, OpenPGP) - too much possibility of mis-use
- Avoid writing your own low-level crypto

Beware of Snake Oil

Snake Oil: bogus commercial cryptographic products.

- **Secret system**: security through obscurity
- **Technobabble**: since cryptography is complicated
- **Unbreakable**: a sure sign of snake oil
- **One-time pads**: a flawed implementation
- **Unsubstantiated "bit" claims**: key lengths are not directly comparable

What cryptography can and can't do

"No one can guarantee 100% security. But we can work toward 100% risk acceptance. ... Strong cryptography can withstand targeted attacks up to a point–the point at which it becomes easier to get the information some other way. ... The good news about cryptography is that we already have the algorithms and protocols we need to secure our systems. The bad news is that that was the easy part; implementing the protocols successfully requires considerable expertise. ... Security is different from any other design requirement, because functionality does not equal quality."

– By Bruce Schneier 1997

A Good Wish

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

– Article 12 Universal Declaration of Human Rights