Practical Aspects of Modern Cryptography

Josh Benaloh
Brian LaMacchia
John Manferdelli

Attacks

- How are cryptosystems typically broken?
  - Back doors
  - Side doors
  - Side windows
  - Crawl spaces
  - …

Side Channel Attacks

Information about a secret key can often be divined by careful observation of a device using the key.

- Timing
- Power Analysis
- Acoustic Emissions
- Cache Usage
- etc.

Timing Attacks

- RSA
  - Each bit of the decryption exponent indicates whether or not to perform a "side multiply".
  - "Chinese remaindering" time varies as the argument crosses from slightly below p to slightly above p.
- AES
  - Selective flushing of cache lines can cause access times to vary depending on key bits.

Protocol Attacks

Hastad Attack on RSA

Given

$$E_1(x) = x^3 \bmod n_1$$

$$E_2(x) = x^3 \bmod n_2$$

$$E_3(x) = x^3 \bmod n_3$$

one can easily compute x.

Protocol Attacks

Bleichenbacher Attack on RSA PKCS#1

PKCS#1 Message Format:

00 01 XX XX ... XX 00 YY YY ... YY

random non-zero bytes

message

Protocol Attacks

If two plaintexts are *ever* encrypted with the same stream cipher and key

$$C_1 = K \oplus P_1$$

$$C_2 = K \oplus P_2$$

an attacker can easily compute

$$C_1 \oplus C_2 = P_1 \oplus P_2$$

from which P_1 and P_2 can be easily teased apart.

Protocol Attacks

- It is easy for an adversary (even one who can't decrypt the ciphertext) to alter the plaintext in a known way.

Bob to Bob's Bank:

Please transfer $0,000,002.00 to the account of my good friend Alice.

Protocol Attacks

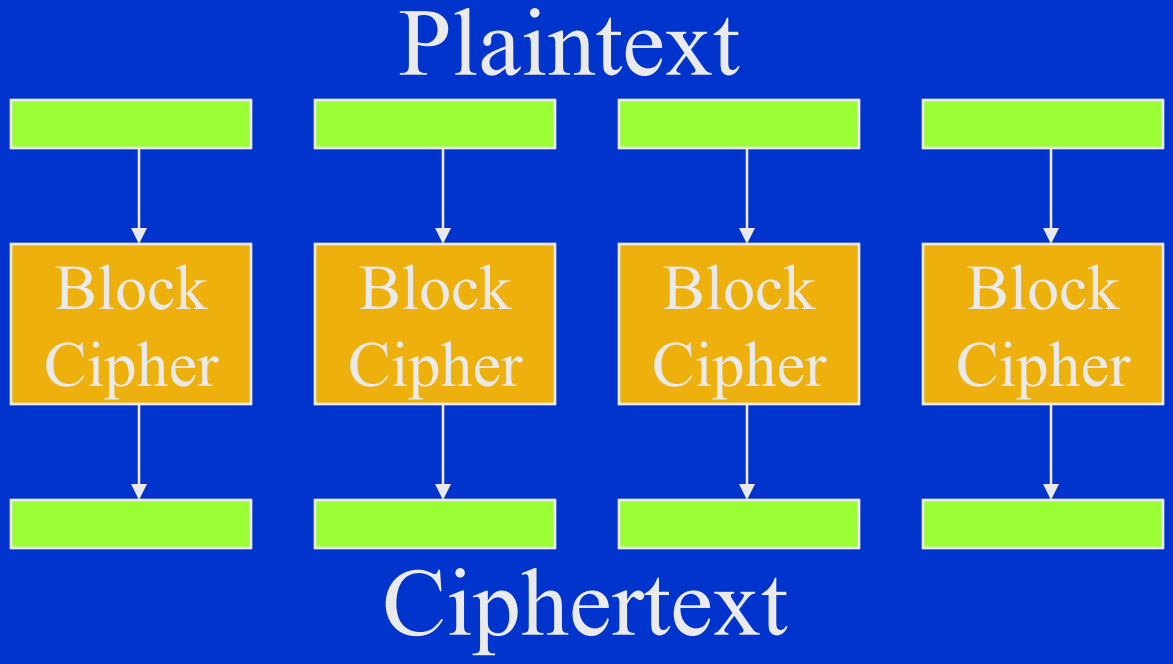
- It is easy for an adversary (even one who can't decrypt the ciphertext) to alter the plaintext in a known way.

Bob to Bob's Bank:

Please transfer $1,000,002.00 to the account of my good friend Alice.

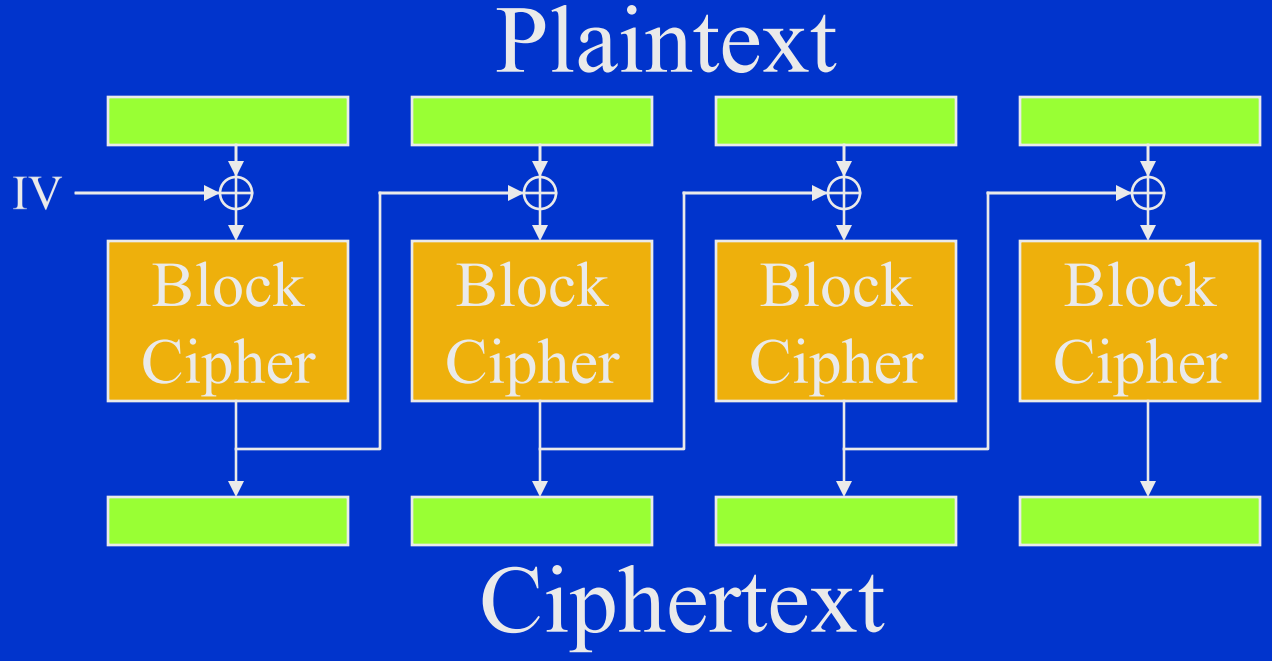
Protocol Attacks

Electronic Code Book (ECB) Encryption



Protocol Attacks

Cipher Block Chaining (CBC) Encryption:



Direct Attacks

Hash Functions

- Find a "low-Hamming-weight differential" Δ (a vector of almost all zeros) such that for messages M, the probability that $h(M \otimes \Delta) = h(M)$ is larger than it should be.

Direct Attacks

Best differential probabilities to date

- MD4: ¼
- MD5: $1/2^{40}$
- SHA-1: $1/2^{63}$

Direct Attacks

Low RSA decryption exponent

- It turns out that if the RSA decryption exponent is less than $n^{1/4}$, then n can be trivially factored given only the encryption exponent.

Direct Attacks

Factoring

- If $n=pq$ – the product of distinct odd primes, then every square modulo n, has four distinct square roots.
- If $y=x^2 \bmod n$, then x and $-x$ are both square roots of y.
- If $y=x^2 \bmod n$, then $y=x^2 \bmod p$ and $y=x^2 \bmod q$.
- There are four ways to "Chinese remainder" $\pm x \bmod p$ with $\pm x \bmod q$.

Direct Attacks

Factoring

- Suppose I have $x_1 \neq \pm x_2$ such that $x_1^2 = x_2^2 \bmod n$.
- Then $x_1 \neq x_2 \bmod p$ and $x_1 \neq -x_2 \bmod q$ (or vice-versa).
- $\mathrm{GCD}(x_1 - x_2, n)$ will therefore produce a non-trivial factor of n.

Direct Attacks

Factoring

- How can I get two distinct values that have the same square modulo n?
- Try, $x \approx \sqrt{n}$, $x \approx \sqrt{2n}$, $x \approx \sqrt{3n}$, …
- If I get, say, $x^2 \bmod n = 49$, I'm really happy.

Direct Attacks

Factoring

- If I get, $x_1^2 \bmod n = 12$ and $x_2^2 \bmod n = 3$, I'm happy too because $(x_1 x_2)^2 \bmod n = 36$.
- In general, look for lots of values x such that $x^2 \bmod n$ is "small" and try to combine the small values to get a square.

Factoring

	2	3	5	7	11	13
x_1^2	1		1			
x_2^2		2		1		
x_3^2	1		2			
x_4^2	2	1		1		1
x_5^2			1		1	
x_6^2		2			1	

Note that $(x_1x_3x_5x_6)^2 = 2^2\times3^2\times5^4\times11^2 = (2\times3\times5^2\times11)^2$.

Lessons

- New attacks must be recognized as a fact of cryptography.
- This makes cryptographic code unique in that a carefully-built, closed system that works perfectly today may become vulnerable tomorrow.
- Cryptographic constructs must be built with agility in mind so that they can be easily updated if and when it becomes necessary.

Thank You