Cryptography vs. Security

Giampaolo Bella

Dipartimento di Matematica e Informatica
Universita` di Catania - ITALY

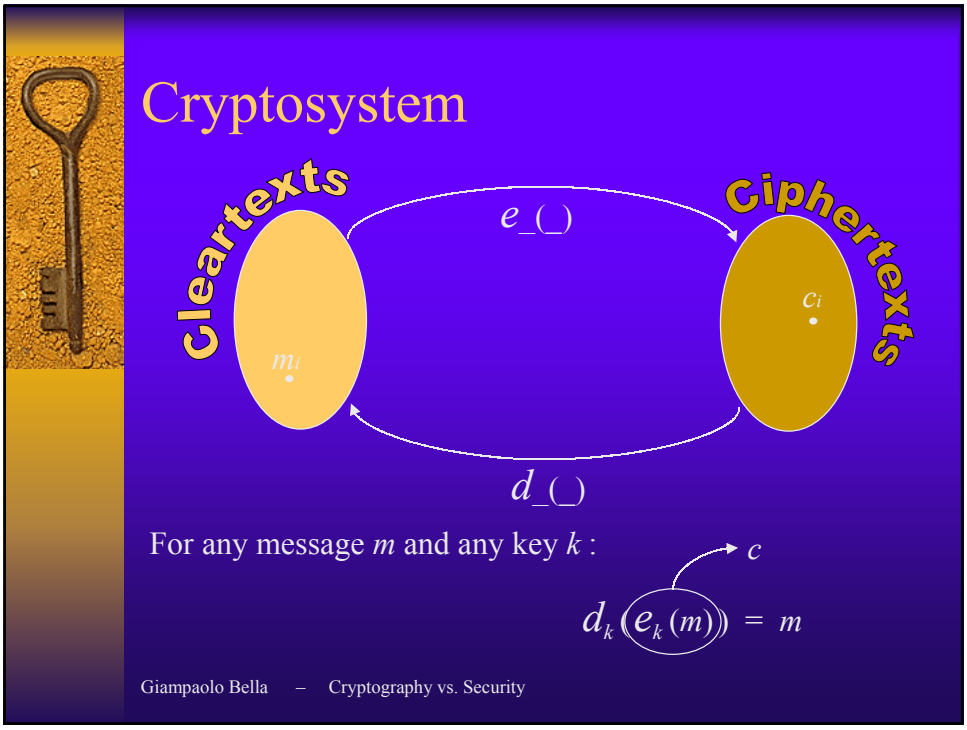
What's Cryptography?

It's the art of *encoding* information…

It's the art of *encoding* and *decoding* information.

Encoded information *may* be unintelligible!


Cryptography
Symmetric
♦ Ancient!
♦ Each agent A has Ka
♦ Ka kept private (shared)
Asymmetric
♦ Recent (late 70's)
♦ A has Ka and Ka-1
♦ Ka-1 kept private, Ka made public
Agents and public keys associated by a hierarchy of certification authorities.
Giampaolo Bella – Cryptography vs. Security


Cryptosystem
Cleartexts
Ciphertexts
e_(_)
mi
ci
d_(_)
For any message m and any key k :
c
dk(ek(m)) = m
Giampaolo Bella – Cryptography vs. Security

RSA (Rivest-Shamir-Adleman, 1978), the most popular asymmetric cryptosystem

- Pick large primes p, q; let $n=p*q$ be public
- Choose r prime with $h(n) = (p-1)*(q-1)$
- Generate s such that $r*s = 1 \bmod h(n)$
- r is the public key; s is the private key
- $e_k(x) = x^k \bmod n$; $\quad d_k(x) = x^k \bmod n$

Can verify that, if x is smaller than n, then

$$d_r(e_s(x)) = x$$

[Exercise. Try *it* with $p=3$, $q=7$, $r=5$, $s=17$ and any input]

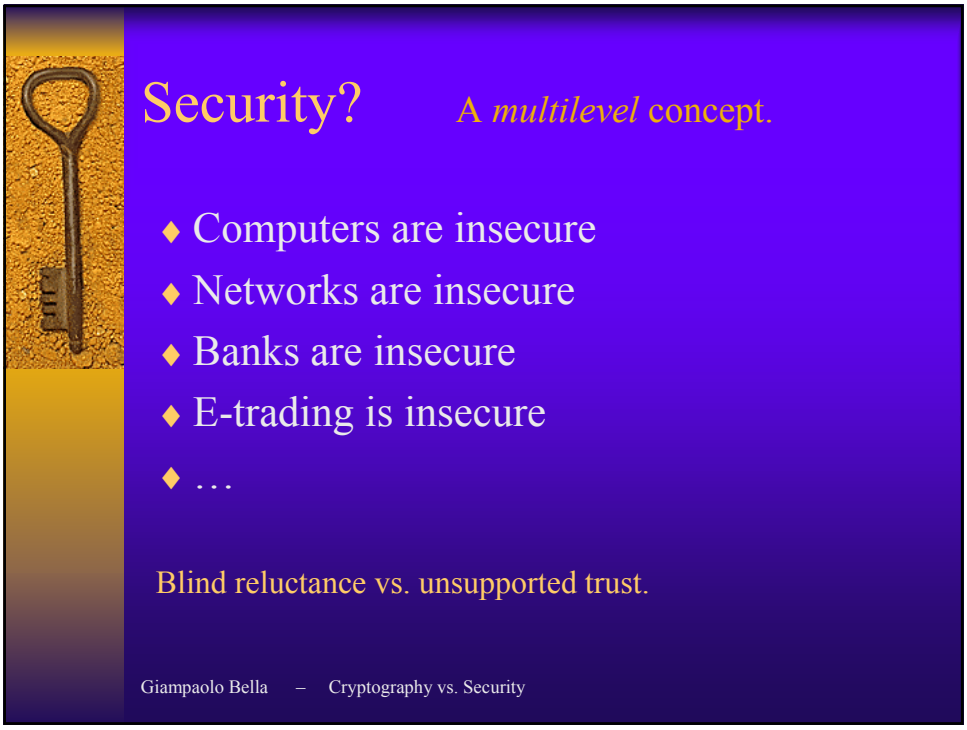
Perfect Cryptography

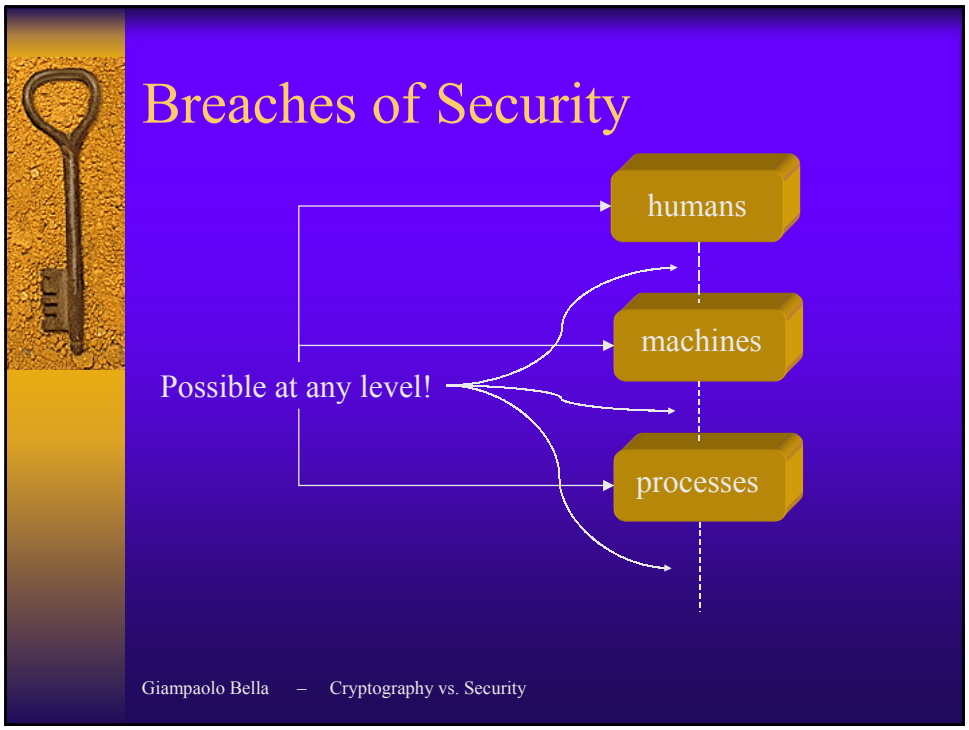
Given $e_K(x)$

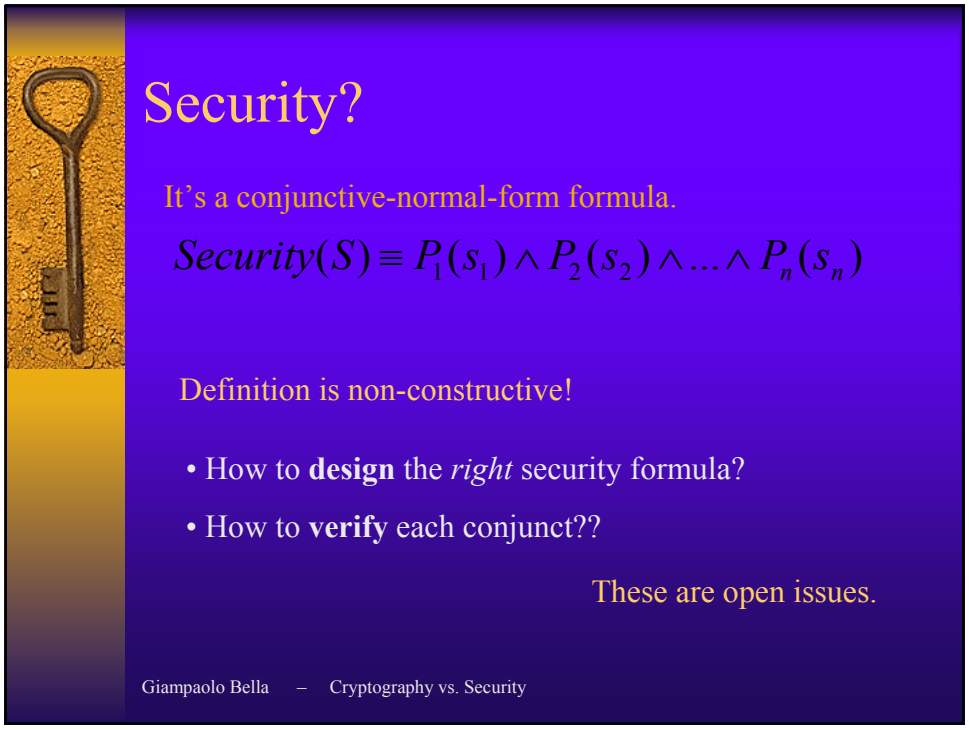
1. K is never at risk
2. x can be obtained iff K is available

Cryptography is rarely perfect in practice!


A Cautionary Tale
The BULL Recursive Protocol (BRL).
♦ Verified assuming perfect crypto (Paulson)
♦ Attacked if crypto is bit-wise XOR (Ryan-Schneider)
Is perfect crypto *the* way to security?
Is perfect crypto *a* way to security?
Giampaolo Bella – Cryptography vs. Security


Security? A *multilevel* concept.
♦ Computers are insecure
♦ Networks are insecure
♦ Banks are insecure
♦ E-trading is insecure
♦ …
Blind reluctance vs. unsupported trust.
Giampaolo Bella – Cryptography vs. Security


Breaches of Security
humans
machines
processes
Possible at any level!
Giampaolo Bella – Cryptography vs. Security


Security?
It's a conjunctive-normal-form formula.
$Security(S) \equiv P_1(s_1) \wedge P_2(s_2) \wedge \ldots \wedge P_n(s_n)$
Definition is non-constructive!
• How to **design** the *right* security formula?
• How to **verify** each conjunct??
These are open issues.
Giampaolo Bella – Cryptography vs. Security

Current focus?

It's on design and verification of the *single* conjunct.

Example.

Secure communication across insecure means.

Tasks.

1. designing a communication protocol that is secure in terms of specific goals;
2. verifying those goals.

Designing a "secure" communication protocol

Might use…

- Steganography – information is *hidden.*

Example:
change the low-order bits of a digital image.

Another application: *digital watermarking.*

Designing a "secure" communication protocol

Might use…

- Chaffing and Winnowing – information is *mixed* to other and then *retrieved* (Rivest).

To winnow: *to separate out or eliminate the poor or useless parts* (Webster's Dictionary).

It is often used when referring to the process of separating grain from chaff.

Scheme used for the goal of *confidentiality*.

Chaffing and Winnowing

- Sender and receiver agree upon a *secret authentication key K*.
- Sender wants to transfer *M*.

  Sender creates a MAC for M concatenated to *K* (by standard algorithms, e.g. HMAC-SHA1).
- Sender transmits pair *M, MAC*(*M,K*).
- Sender adds *chaff*: sends a number of bogus pairs (fake messages with random, potential MAC's).
- Receiver *winnows* the flow: checks all pairs for matching components.

Confidentiality of *M* only depends on strength of MAC.

No cryptography used.

Designing a "secure" communication protocol

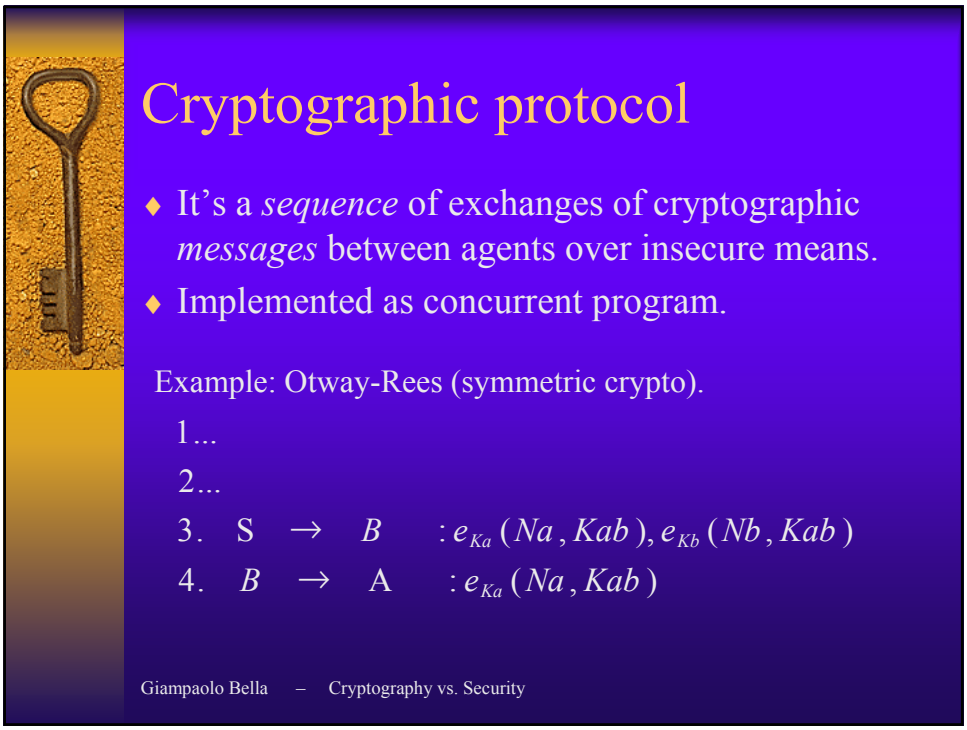
Might use…

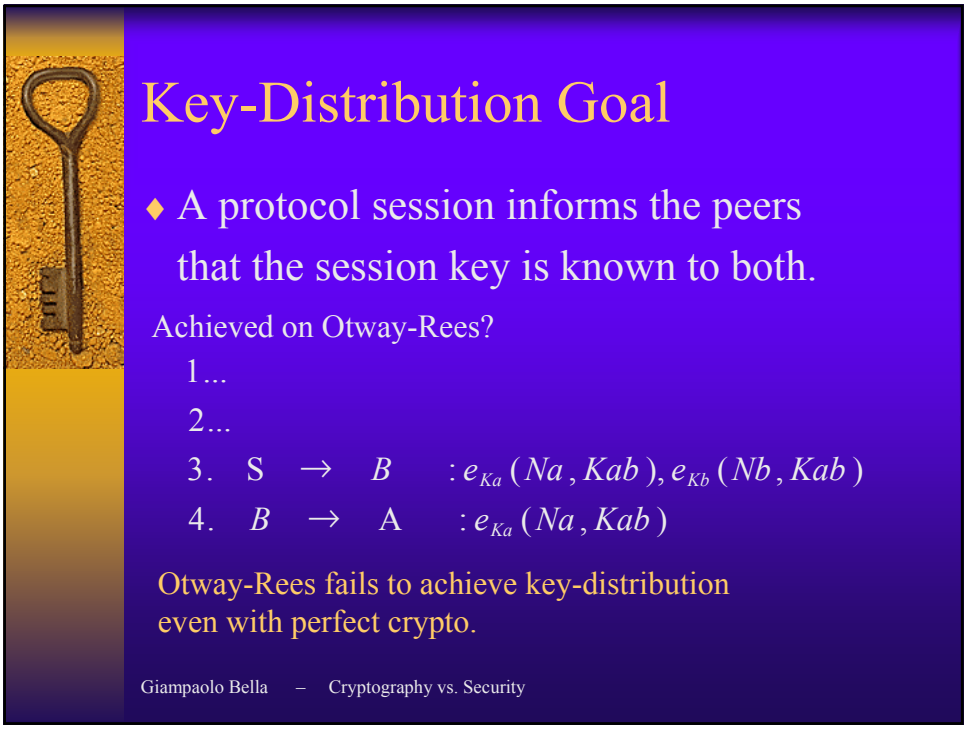
- Steganography – information is *hidden.*
- Chaffing and Winnowing – information is *mixed* to other and then *retrieved.*
- Cryptography – information is *encoded* and then *decoded.*

What we learn

1. Cryptography is not *the only* way to security.
2. It is in fact *a* way to achieve "a portion" of security, which has to do with communication.

Who said 2?


Cryptographic protocol
♦ It's a *sequence* of exchanges of cryptographic *messages* between agents over insecure means.
♦ Implemented as concurrent program.
Example: Otway-Rees (symmetric crypto).
1...
2...
3. S → B : $e_{Ka}(Na, Kab), e_{Kb}(Nb, Kab)$
4. B → A : $e_{Ka}(Na, Kab)$
Giampaolo Bella – Cryptography vs. Security


Key-Distribution Goal
♦ A protocol session informs the peers that the session key is known to both.
Achieved on Otway-Rees?
1...
2...
3. S → B : $e_{Ka}(Na, Kab), e_{Kb}(Nb, Kab)$
4. B → A : $e_{Ka}(Na, Kab)$
Otway-Rees fails to achieve key-distribution even with perfect crypto.
Giampaolo Bella – Cryptography vs. Security

Fixing Otway-Rees

3. S $\rightarrow$ B : $e_{Kb}(Na, Kab, e_{Ka}(Nb, Kab))$
4. B $\rightarrow$ A : $e_{Ka}(Na, Kab)$

Cryptography must be used cautiously.

The Woo-Lam Protocol

- Uses symmetric crypto.
- Aims at *authentication of A with B.*

1. A $\rightarrow$ B : A
2. B $\rightarrow$ A : Nb
3. A $\rightarrow$ B : $e_{Ka}(Nb)$
4. B $\rightarrow$ S : $e_{Kb}(A, e_{Ka}(Nb))$
5. S $\rightarrow$ B : $e_{Kb}(Nb)$

An attack on Woo-Lam

1. $C \rightarrow B : A$
1'. $C \rightarrow B : C$

2. $B \rightarrow A : Nb$
2'. $B \rightarrow C : Nb'$

3. $C \rightarrow B : e_{Kc}(Nb)$
3'. $C \rightarrow B : e_{Kc}(Nb)$

4. $B \rightarrow S : e_{Kb}(A, e_{Kc}(Nb))$
4'. $B \rightarrow S : e_{Kb}(C, e_{Kc}(Nb))$

5. $S \rightarrow B : e_{Kb}(Nb'')$
5'. $S \rightarrow B : e_{Kb}(Nb)$

Serious failure of authentication!

Conclusions

- Cryptography **might** be **a** way towards security.
- Research towards perfect cryptography isn't all that's needed.
- Verifying a single security goal may be daunting.
- Security is a vague target yet.