A Dot.Com Security Problem:

Understand how Encryption and Digital Signatures Work

2-318

Rafal Lukawiecki
rafal.lukawiecki@uk.aris.com
Strategic Consultant
Aris Corp

Microsoft®

Tech·Ed 2000

It's time to **Build** the

Business Internet

Supported by

COMPAQ

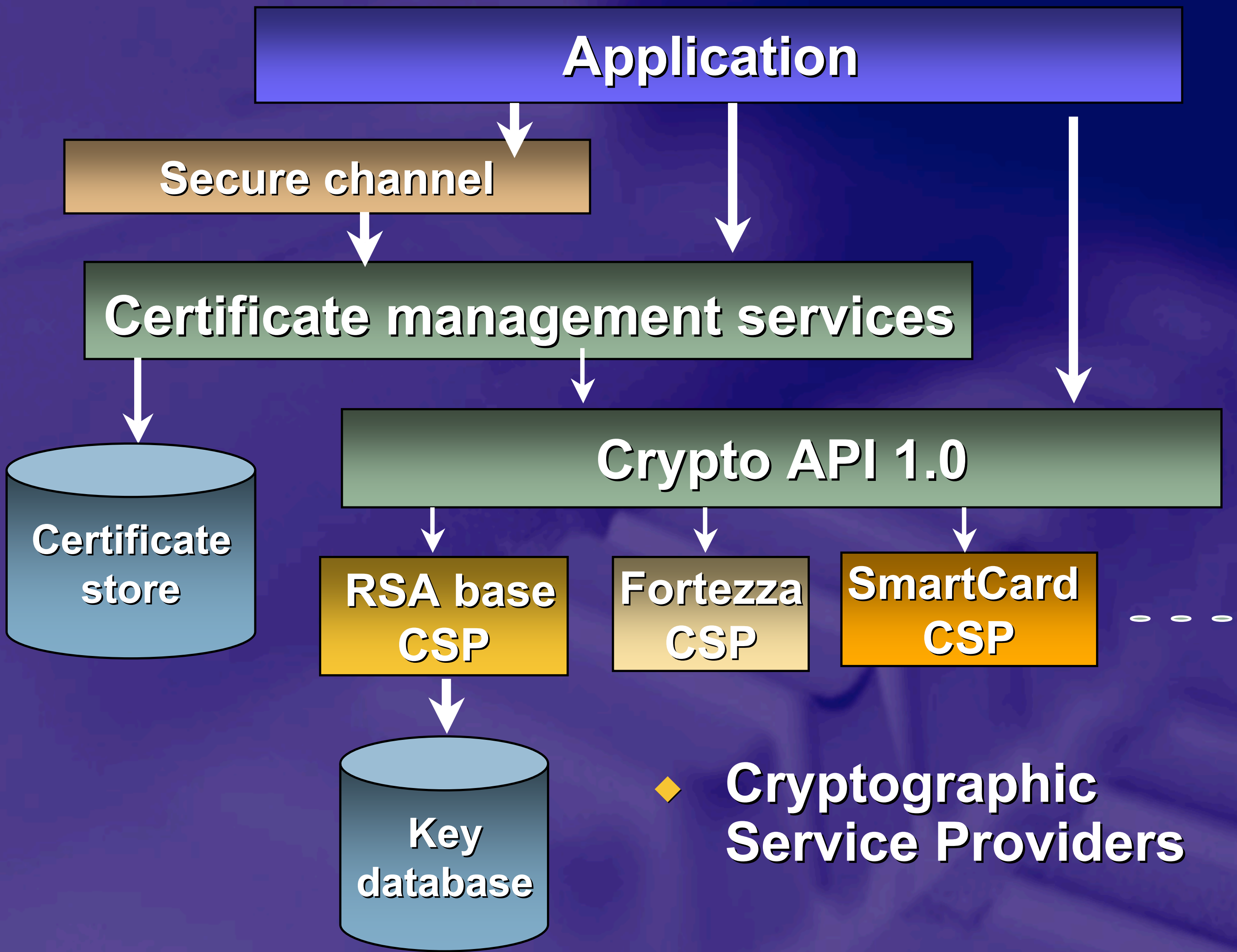
Agenda

- What is Good and What is Bad?
- How does it work?
- Breaking it
- Security recommendations

What is Really Secure?

- Look for systems
  - From well-know parties
  - With published (not secret!) algorithms
  - That generate a lot of interest
  - That have been hacked for a few years
  - That have been analysed mathematically
- Absolutely do not "improve" algorithms yourself
- Employ someone to attempt a break-in

Crypto API Architecture



- Cryptographic Service Providers

Basic Terminology

- Plaintext
  - The stuff you want to secure, typically readable by humans (email) or computers (software, order)
- Ciphertext
  - Unreadable, secure data that must be decrypted before it can be used
- Key
  - You must have it to encrypt or decrypt (or do both)
- Cryptoanalysis
  - Hacking it by using science
- Complexity Theory
  - How hard is it and how long will it take to run a program

Symmetric Key Cryptography

Plain-text input

"The quick brown fox jumps over the lazy dog"

Encryption

Cipher-text

"AxCv;5bmEseTfid3)fGsmWe#4^,sdgfMwir3:dkJeTsY8R\s@!q3%"

Decryption

Plain-text output

"The quick brown fox jumps over the lazy dog"

Same key (shared secret)

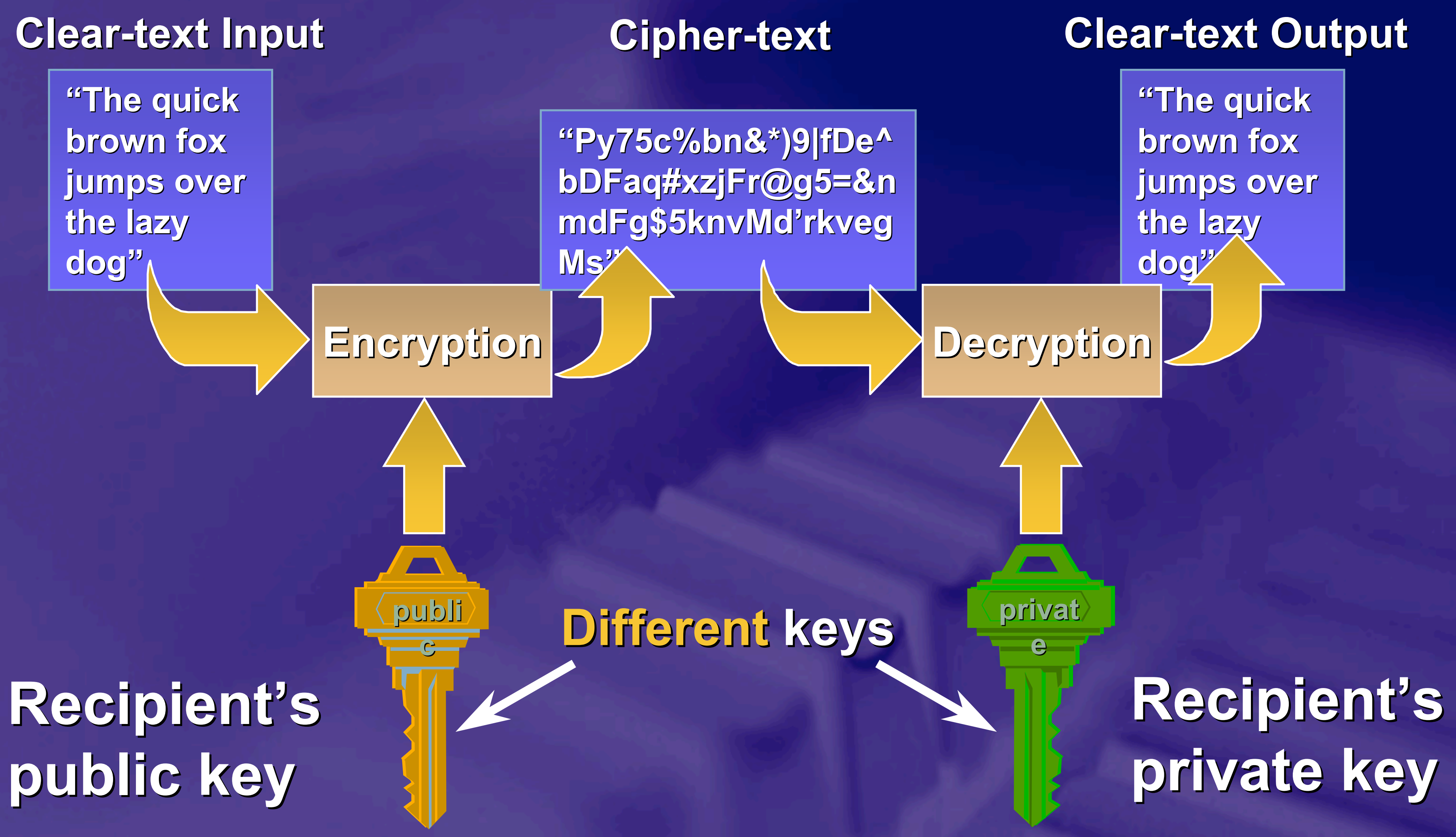
Symmetric Pros and Cons

- **Weakness:**
  - Agree the key beforehand
  - Securely pass the key to the other party
- **Strength:**
  - Simple and really very fast (order of 1000 to 10000 faster than asymmetric mechanisms)
    - Super-fast if done in hardware (DES)
    - Hardware is more secure than software, so DES makes it really hard to be done in software, as a prevention

Public Key Cryptography

- Knowledge of the *encryption* key doesn't give you knowledge of the *decryption* key
- Receiver of information generates a pair of keys
  - Publish the public key in directory
- Then anyone can send him messages that only she can read

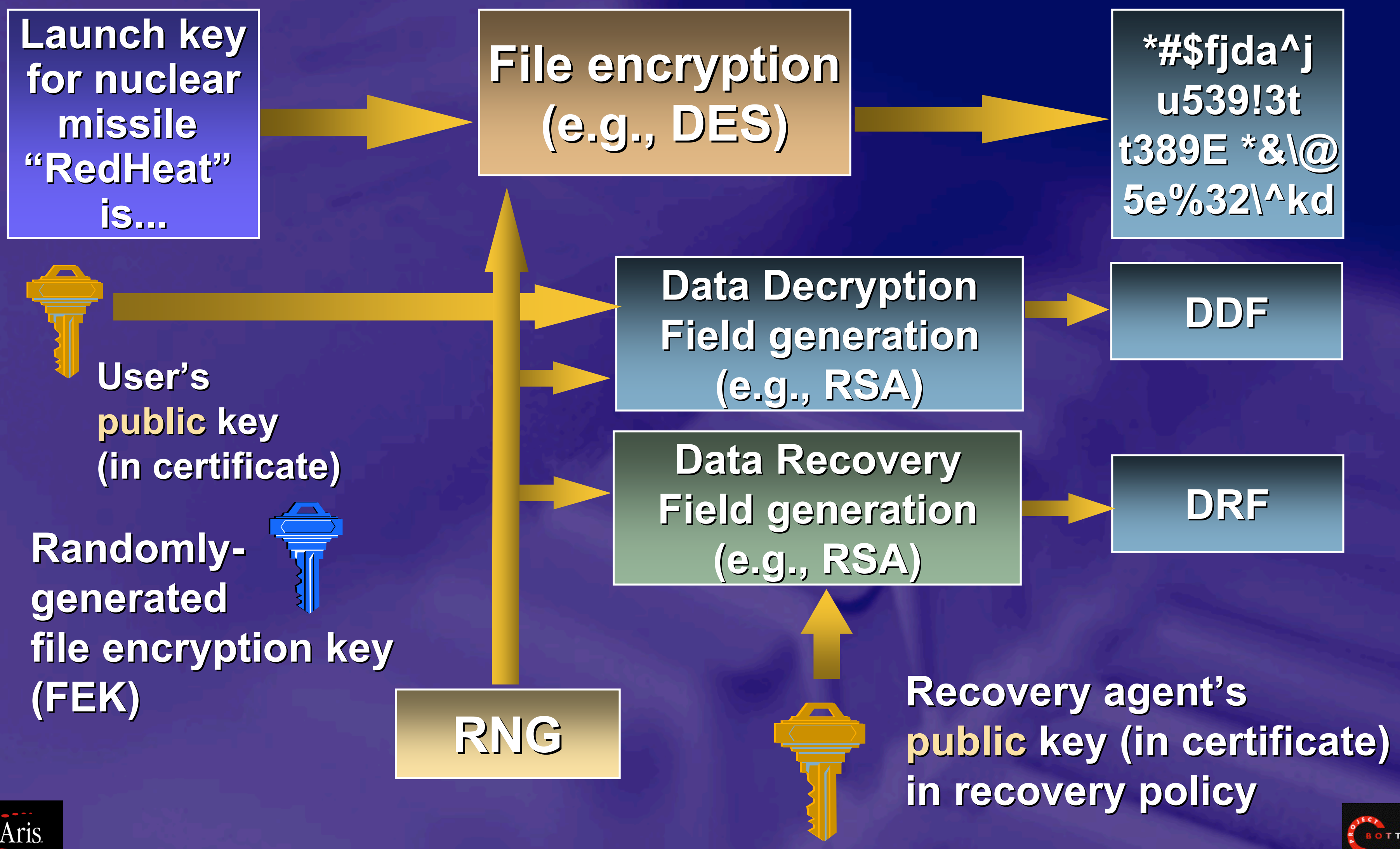
Public Key Encryption



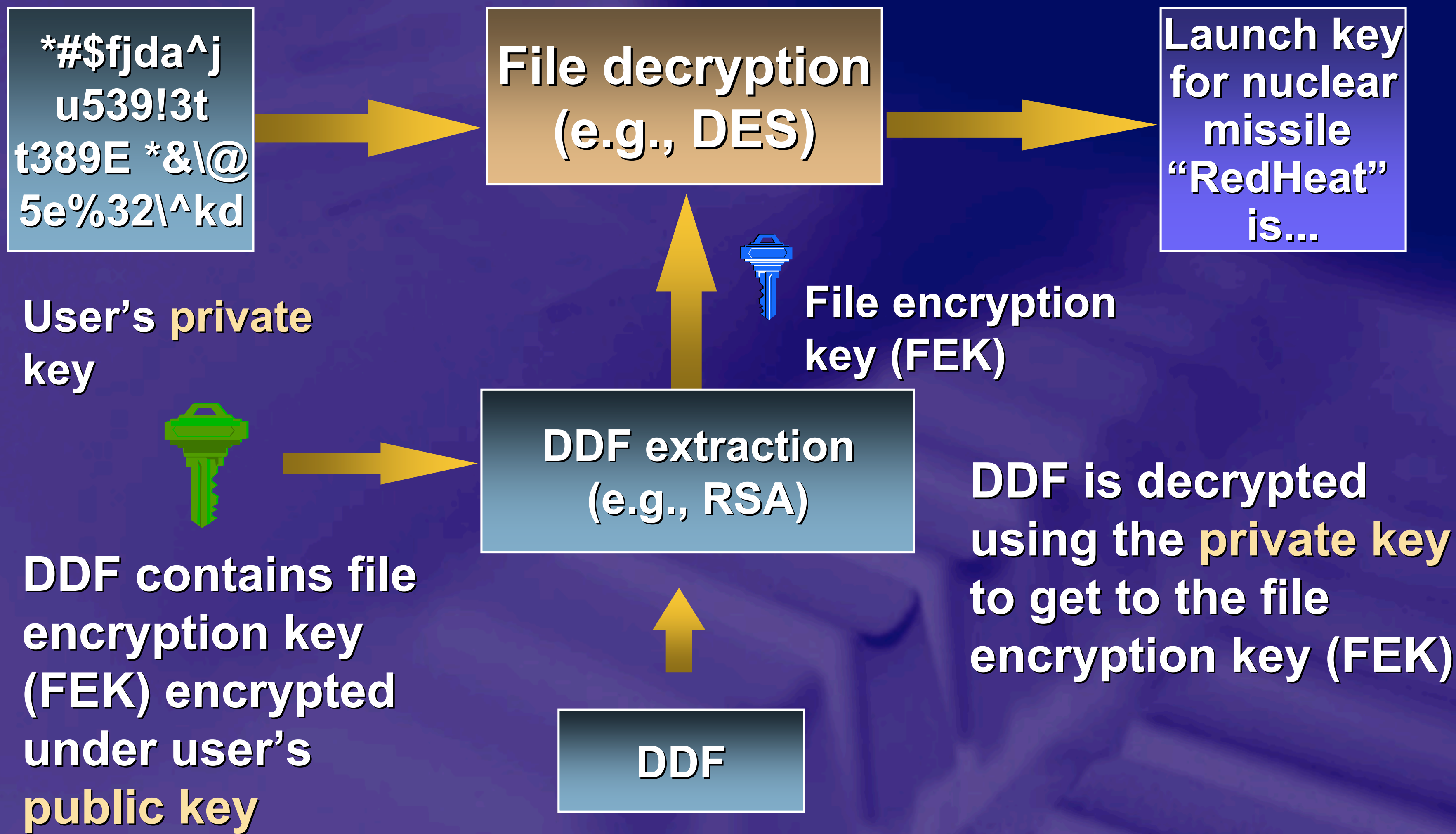
Problem of Key Recovery

- What if you lose the private key? ☺
- Data recovery by authorized agents
  - Integrated key management
- Windows 2000:
  - Flexible recovery policy
    - Enterprise, domain, or per machine
  - Encrypted backup and restore
    - Integrated with Windows NT backup
- Potential weakness but you can opt not to use it!

Data Encryption Process



Data Decryption Process



Data Recovery Process

*#$fjda^j
u539!3t
t389E *&\@
5e%32\^kd

File decryption
(e.g., DES)

Launch key
for nuclear
missile
"RedHeat"
is...

Recovery agent's
private key

File encryption
key (FEK)

DRF extraction
(e.g., RSA)

DRF

DRF contains file encryption key (FEK) encrypted under recovery agent's **public key**

DRF is decrypted using the **private key** of recovery agent to get to the file encryption key (FEK)

Digital Signatures

- Want to give plain text data to someone, and allow them to verify the origin
- Hash the text, encrypt the hash, provide the signature with the plain text
  - Encrypt (Hash(plain text))
  - Encrypt the hash using Private key
- Recipient
  - Hashes plain text: H(pt)
  - Decrypts D(E(H(pt)) = H(pt) using Public key
  - Compares the result!

Digital Signatures

- What does it all give us?
- We know exactly who signed it
  - Stronger than written sigs in terms of proving it
  - Legally binding in US and soon in EU
- Even a minor change to the document after signing is immediately known

Hold-on to your seats…

Quick overview of all major algorithms

DES, IDEA, RC2, RC5

- Symmetric
- DES (Data Encryption Standard) is the most popular
  - NSA may know "back door" - not very likely considering 20 years research
  - Keys very short: 56 bits
  - Triple DES (3 DES) not much more secure but may thwart NSA

S/MIME, SSL, Kerberos

- IDEA (International Data Encryption Standard)
  - Similar to DES, but "not" from NSA
  - 128 bit keys

PGP

- RC2 & RC5 (by R. Rivest)
  - RC2 is older and RC5 newer (1994) - similar to DES and IDEA

S/MIME, SSL

RC4

- Symmetric
  - Fast, streaming encryption
- R. Rivest in 1994
  - Originally secret, but “published” on sci.crypt
- Related to “one-time pad”, theoretically most secure
- *But!*
- It relies on a really good random number generator
  - And that is the problem

PPTP

RSA, ElGamal

- Asymmetric
  - Very slow and computationally expensive – need a computer
  - Very secure
- Rivest, Shamir, Adleman – 1978
  - Popular and well researched
  - Strength in *today's* inefficiency to factorise into prime numbers
  - Some worries about key generation process in some implementations
- ElGamal
  - Relies on complexity of discreet logarithms

SSL, PGP

MD5, SHA

- Hash functions – not encryption at all!
- Goals:
  - Not reversible: can't obtain the message from its hash
  - Hash much shorter than original
  - Two messages won't have the same hash
- MD5 (R. Rivest)
  - 512 bits hashed into 128
  - Mathematical model still unknown
  - But it resisted major attacks
- SHA (Secure Hash Algorithm)
  - US standard based on MD5

S/MIME, SSL, PGP, Digital Sigs

Diffie-Hellman, “SSL”, Certs

- Methods for key exchange
- DH is very clever since you always generate a new “key-pair” for each asymmetric session
  - STS, MTI, and certs make it even safer
- SSL uses a protocol to exchange keys safely (see later)
- Certs (certificates) are the most common way to exchange public keys
  - Foundation of Public Key Infrastructure (PKI)

PGP

Everyone

X.509v3 Certificates

- Simple and powerful way of ensuring that a public key belongs to whom it claims to belong to
- Cert contains:
  - Your public key
  - Data about you (X.400/500 format)
  - Digital signature of someone known by everyone: CA
    - Certificate Authorities, such as Verisign, Thawte, BT, C&W and many others
  - Passed in PKCS “envelopes”, e.g. #7

S/MIME,

SSL

Aris

PROJECT BOTTICELLI

PGP and S/MIME

- Pretty Good Privacy – well known personal privacy package
  - Uses IDEA, Diffie-Hellman and RSA
  - Not subject to US and other limitations
  - Key management is not too easy
  - Integrates well with Microsoft Outlook
- S/MIME – standard supported by all
  - Uses DES, 3DES or RC2 and MD5 or SHA1
  - Subject to export limitations (obsolete)
  - Windows 2000 helps with keys
  - Supported by Exchange, Outlook (& Express), Netscape and many others

SSL – Secure Sockets Layer

- Secures internet traffic
  - Uses similar protocols to S/MIME
  - Asymmetric key exchange, symmetric encryption
- Solves key exchange problem
  - *Client Hello* – have some random stuff
  - *Server Hello* – here is my random stuff
  - *Server Cert* – it's me, your bank!
  - *Server Key Exchange*
    - Here is a secret encrypted with your public key (or let's use DH etc.)
    - Let's make the secret better by hashing it many times with both MD5 and SHA
  - *Cert Verify*

Web, TCP/IP

Looking After Keys

- Your private key is YOU!
- Store securely
  - On your machine in *Protected Storage* service on Windows 2000 and in IE
  - Best: on smartcards designed for it
- Have a way of revoking them
- Trust managed by PKI
- Weakness: it all relies on passwords, PINs etc…

Cryptoanalysis

- Brute force
  - Good for guessing passwords, and some 40-bit symmetric keys (in some cases needed only 2^7 attempts)
- Frequency analysis
  - For very simple methods only (US mobiles)
- Linear cryptoanalysis
  - For stronger DES-like, needs 2^{43} plain-cipher pairs
- Differential cryptoanalysis
  - Weaker DES-like, needs from 2^{14} pairs

Strong Systems

- It is always a mixture! Changes all the time…
- Symmetric:
  - Min. 128 bits for RC2 & RC5, 3DES, IDEA, carefully analysed RC4
- Asymmetric:
  - RSA, ElGamal, Diffie-Hellman (for keys) with minimum 1024 bits (go for the *maximum*, typically 4096)
- Hash:
  - Either MD5 or SHA but with *at least* 128 bit results

Weak Systems

- Anything with 40-bits (including 128 and 56 bit versions with the remainder “fixed”)
- CLIPPER
- A5 (GSM mobile phones)
- Vigenère (US mobile phones)
  - Dates from 1585!
- Unverified certs with no trust
- Weak certs (as in many “class 1” personal certs)

Recommendations

- Do not rely on new and untested or proprietary systems
  - E.g. consider migration to L2TP for VPN on Windows 2000
- Build your PKI and secure, secure, secure your master root keys
- Implement key revocation strategy
- Start using good smartcard systems
- Oh dear, good passwords again…

Call To Action

- Visit www.microsoft.com/security
- Obtain certificates and experiment with them – appoint an internal security consultant
- Attend sessions on PKI and Active Directory Security
- Obtain 3rd party tools, such as PGP
- For more detail, read:
  - *Applied Cryptography*, B. Schneier, John Wiley & Sons, ISBN 0-471-12845-7
  - *Foundations of Cryptography*, O. Goldereich, www.eccc.uni-trier.de/eccc-local/ECCC-Books/oded_book_readme.html
  - *Handbook of Applied Cryptography*, A.J. Menezes, CRC Press, ISBN 0-8493-8523-7

Aris

Stand G27

Aris instructs, **develops,**
deploys, *consults,*
optimises, designs,
teaches

Thank You!

Aris Consulting (MS SP Partner Tier 1)

Aris Education (MS CTEC)

Stand G27

www.aris.com

Consultants and Trainers to:

Microsoft, Schroders, General Electric, NATO, NASDAQ, PricewaterhouseCoopers, Reuters, Rover, Channel 4, BAA, Boeing, Credit Suisse, Polygram, NatWest, Slaughter & May, British Telecom, IBM, Aspect Telecommunications, Marriott, Interflora, Loot, Hamleys, Ministry of Sound, Datacash, Acordis, NHS, GlaxoWellcome, Inland Revenue…

Microsoft® Tech·Ed 2000

Where do you want to go today?®