暗号／情報セキュリティ

ー暗号アルゴリズムの標準化を中心にー

2002年7月5日

三菱電機情報技術総合研究所
松井　充　matsui@iss.isl.melco.co.jp

古典暗号から現代暗号へ

- 古典暗号の世界
  - 暗号の歴史は人類の歴史と同じ長さ
  - 軍事外交目的の非公開技術
  - 参加者限定の１対１通信を前提
  - 文字の置換を中心とする変換処理
  - 安全性評価は文字の出現頻度の統計学
- 現代暗号の世界
  - 本格的に開かれた研究は１９７０年代から
  - プライバシー保護という動機付け
  - 不特定多数が参加するネットワーク指向
  - ディジタル信号の変換処理
  - 計算量理論との融合

現代暗号のコンセプト

- 非公開技術から公開技術への転換
  - 1976年　米国政府標準暗号DESの制定と仕様公開
  - 1978年　公開鍵暗号の発明⇒ﾈｯﾄﾜｰｸ暗号の実現
- 暗号方式の公開が定着へ
  - 第三者の安全性検証による信頼性向上
  - 暗号の健全利用の促進
- 電子社会の見えざるインフラに
  - ディジタル情報保護のために不可欠な道具
  - キーワードは「Privacy」と「Money」

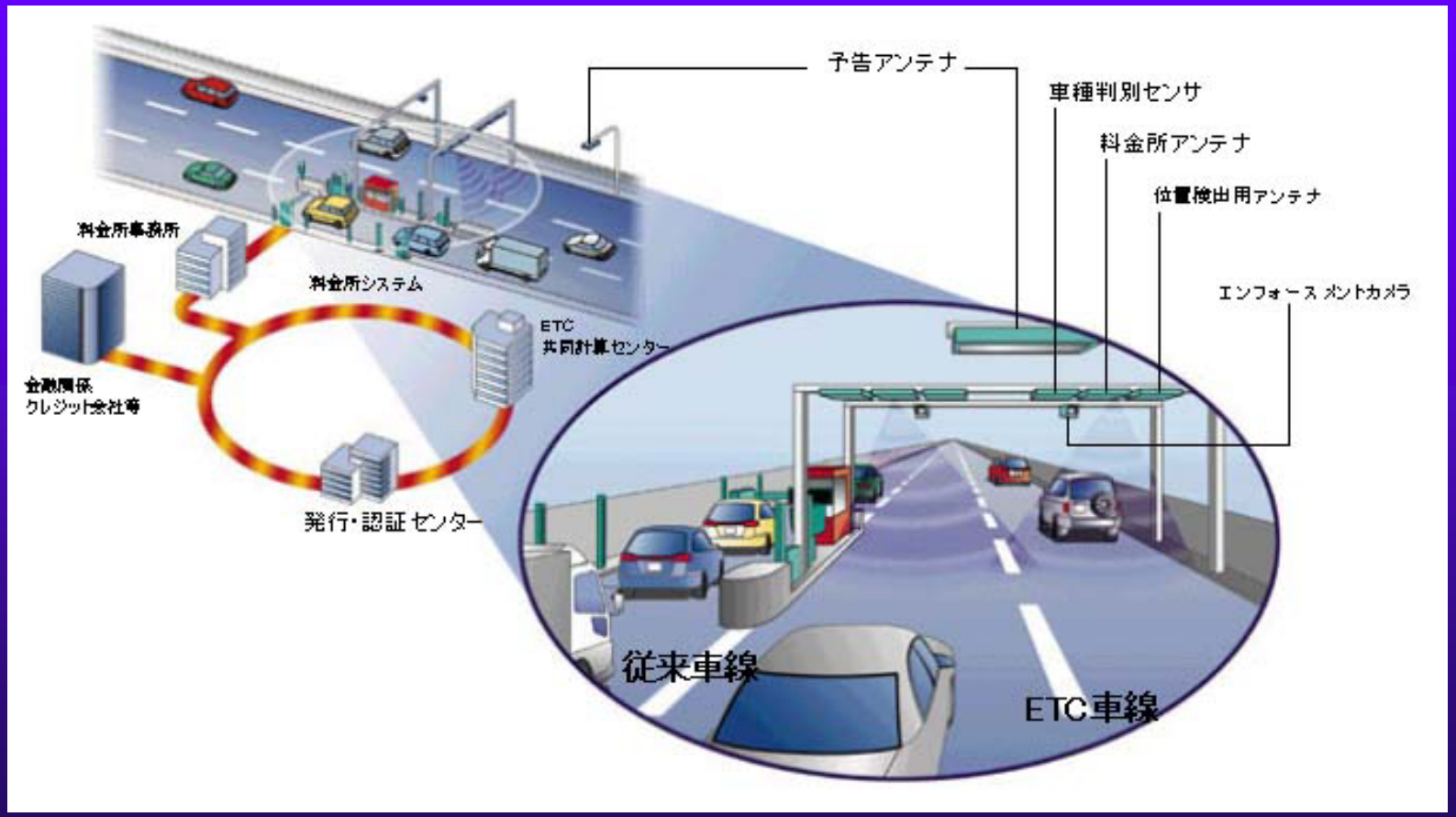
暗号技術の利用例（1）

ETC (Electric Toll Collection) System

●ノンストップ＆キャッシュレスを実現するETCは、数々の効果を発揮するものと期待されている

三菱電機ホームページ http://www.melco.co.jp より

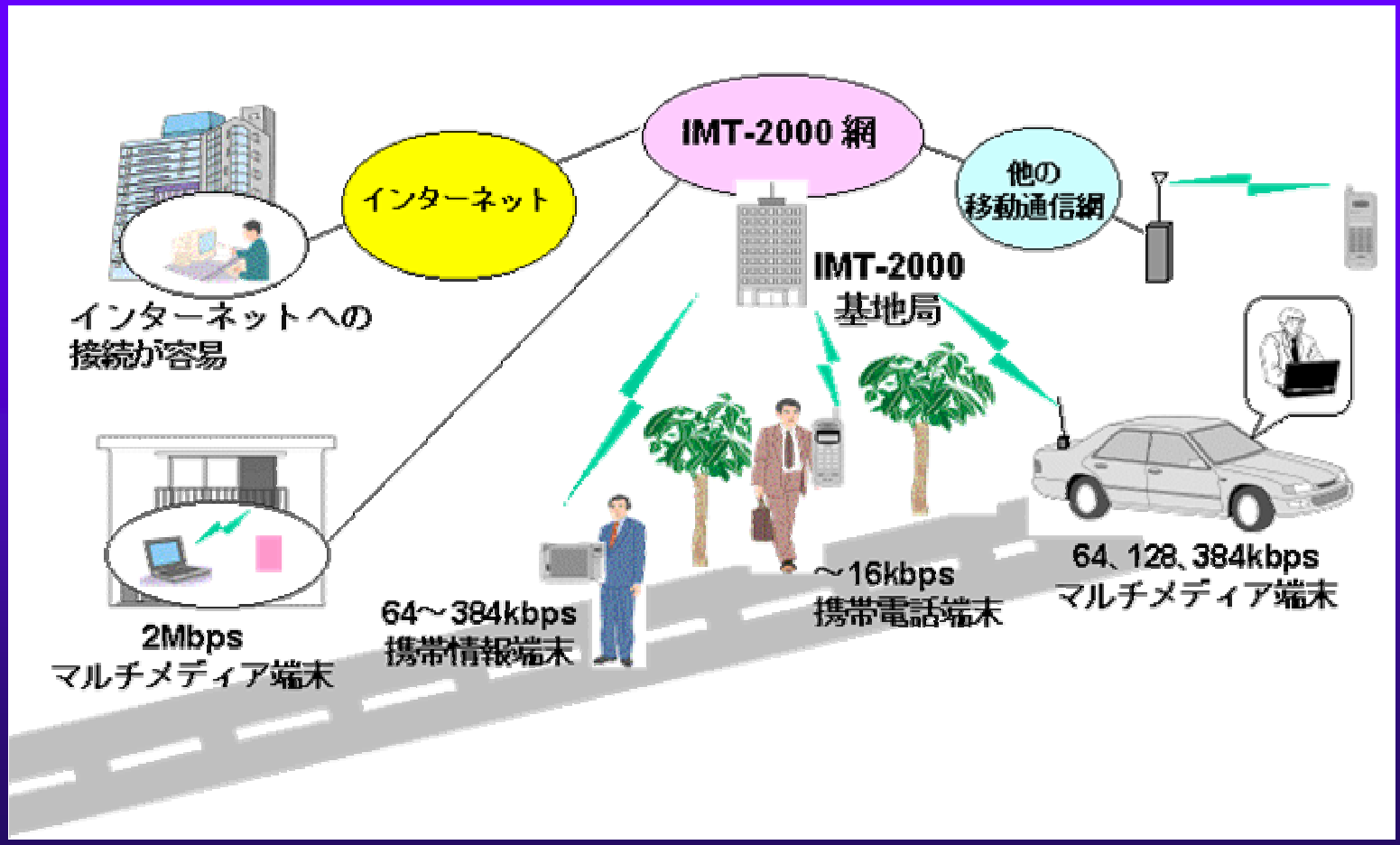
ETC (Electric Toll Collection) System



三菱電機ホームページ http://www.melco.co.jp より

暗号技術の利用例（2）

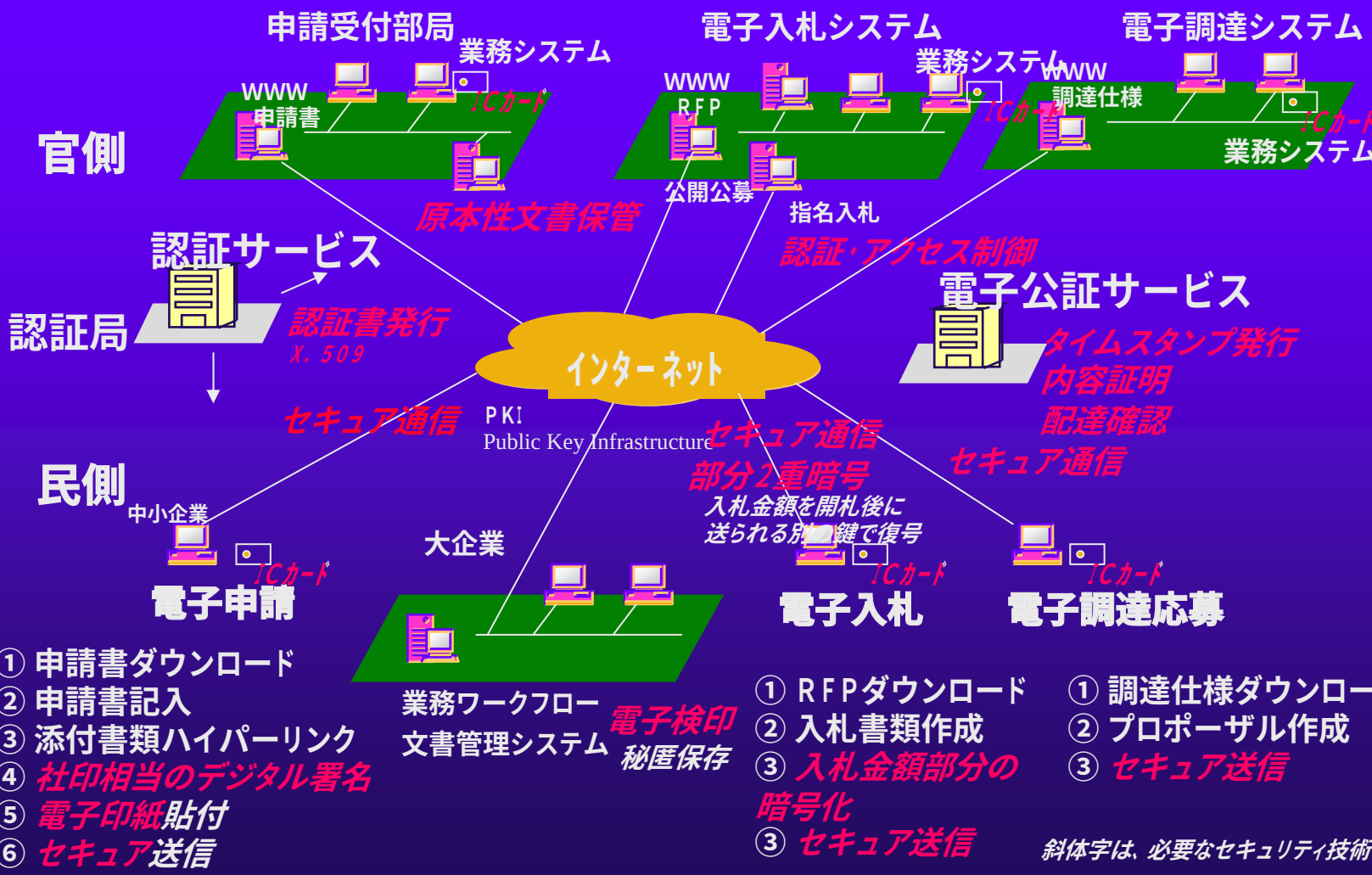
次世代携帯電話（W-CDMA System）



郵政省：第三世代移動通信システム（IMT-2000）の導入に向けて：1999年12月10日発表

暗号技術の利用例（3）

電子申請･調達･入札



① 申請書ダウンロード
② 申請書記入
③ 添付書類ハイパーリンク
④ *社印相当のデジタル署名*
⑤ *電子印紙貼付*
⑥ *セキュア送信*

① ＲＦＰダウンロード
② 入札書類作成
③ *入札金額部分の暗号化*
③ *セキュア送信*

① 調達仕様ダウンロー
② プロポーザル作成
③ *セキュア送信*

斜体字は、必要なセキュリティ技術

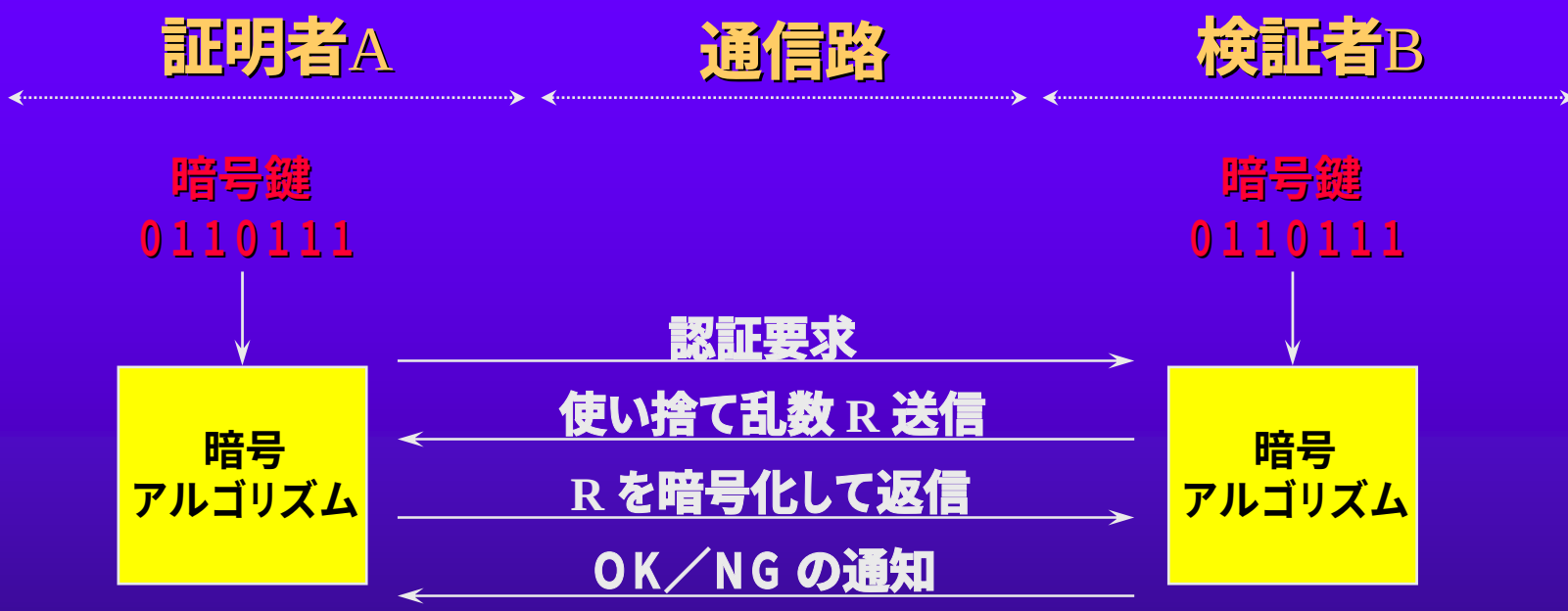
暗号方式の分類

- **共通鍵暗号（秘密鍵暗号，対称鍵暗号）**
  - 送信者と受信者が共通の鍵をもつ
  - 小型・高速であることにその存在価値
  - (例)　DES, RIJNDAEL, MISTY, KASUMI
- **公開鍵暗号（非対称鍵暗号）**
  - 暗号化の鍵と復号の鍵が異なる特殊な仕掛けが必要
  - ディジタル署名や鍵配送など応用が豊富、但し低速
  - (例) RSA, DSA, 楕円暗号

共通鍵暗号の原理

- 暗号化の鍵と復号の鍵が同じ（これを秘密鍵と呼ぶ）
- 秘密鍵は事前に何らかの方法で共有しておく必要がある

共通鍵暗号によるユーザ認証



- パスワード（暗号鍵）を通信路に流すことなく認証が可能
- A が乱数を生成して B に暗号化させることにより、相互認証も可能となる

代表的な共通鍵暗号（1）

DES (Data Encryption Standard)

- 米国政府（商務省）が共通鍵暗号の公募
- ＩＢＭが応募したものがＤＥＳの原形
- ＮＳＡ（National Security Agency）が評価および改良
- １９７６年ＦＩＰＳ（連邦政府情報処理標準）として成立
- １９８１年ＡＮＳＩに採用
- ＩＳＯでの標準化は米国自身が拒否

- デファクト共通鍵暗号として世界中で利用
- 計算機の進歩の結果 DES はもはや安全ではない
- 現在 Triple-DES が急速に浸透中
- NIST は新暗号の標準化を目指す ⇒ AES

DES Algorithm

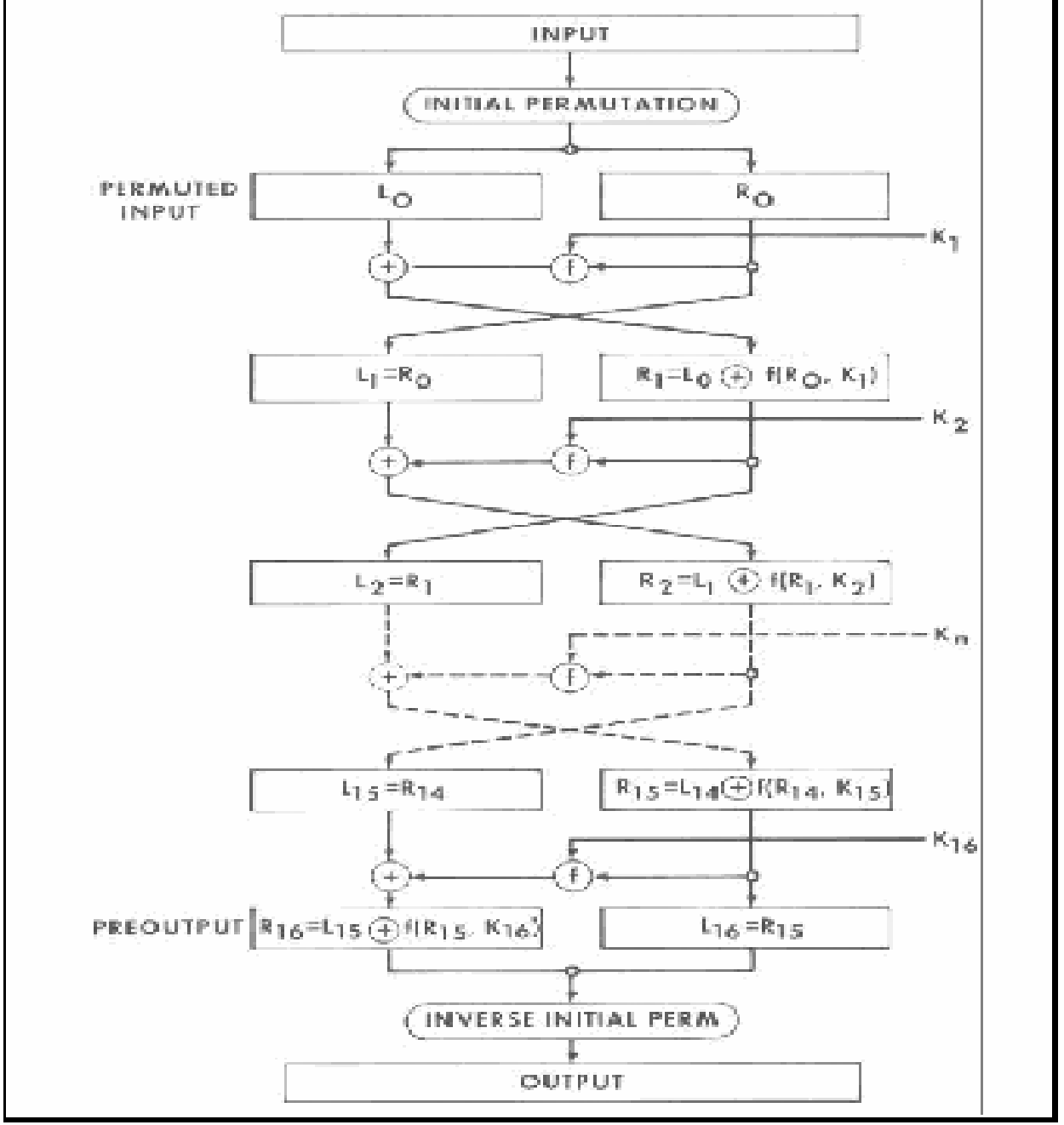


Figure 1. Enciphering computation

代表的な共通鍵暗号（2）

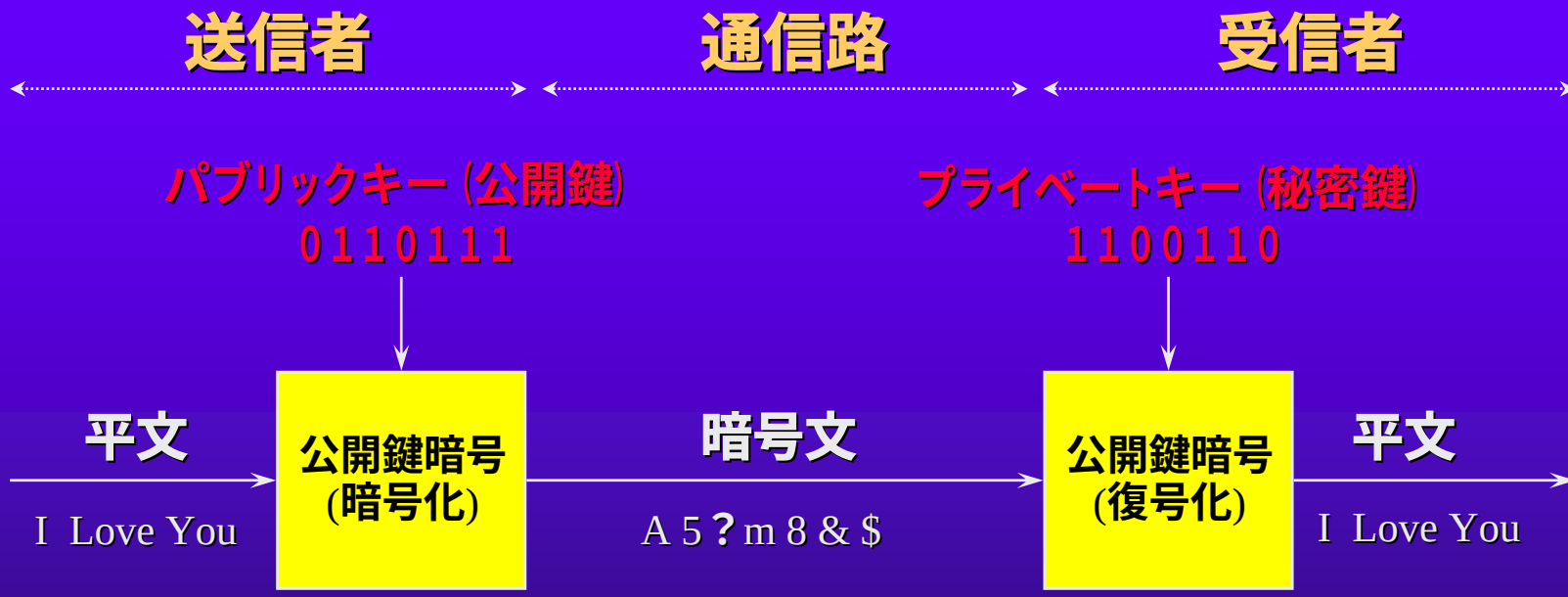
AES (Advanced Encryption Standard)

- DES の後継共通鍵暗号を選定する米国のプロジェクト
- NIST（商務省の組織）が主催する公募によって選定
- 選定されたアルゴリズムは FIPS に登録
- １９９７年1月AESプロジェクト開始
- 世界各国から１５個の暗号方式が提案された
- 第１次選考で５本に絞られた（１９９９年８月）
  米国提案３本、欧州提案２本
- 最終選考で選ばれたのはベルギー製のRIJNDAEL
- AES の Official Home Page
  http://csrc.ncsl.nist.gov/encryption/aes/aes_home.htm

AES のインパクトと今後

- 欧州の候補がAESに選定された
  - 政治的には意外，技術的には当然
- 将来世界のデファクト標準共通鍵暗号に
  - アメリカ政府公認，ライセンスフリー
- Triple-DES との住み分けは？
  - AES の本格的な普及は3～5年後
- 日本標準暗号は必要か
  - 必要との認識が多数　ただし決定機関なし
- Target Specific Cipher は生き残る

公開鍵暗号の原理



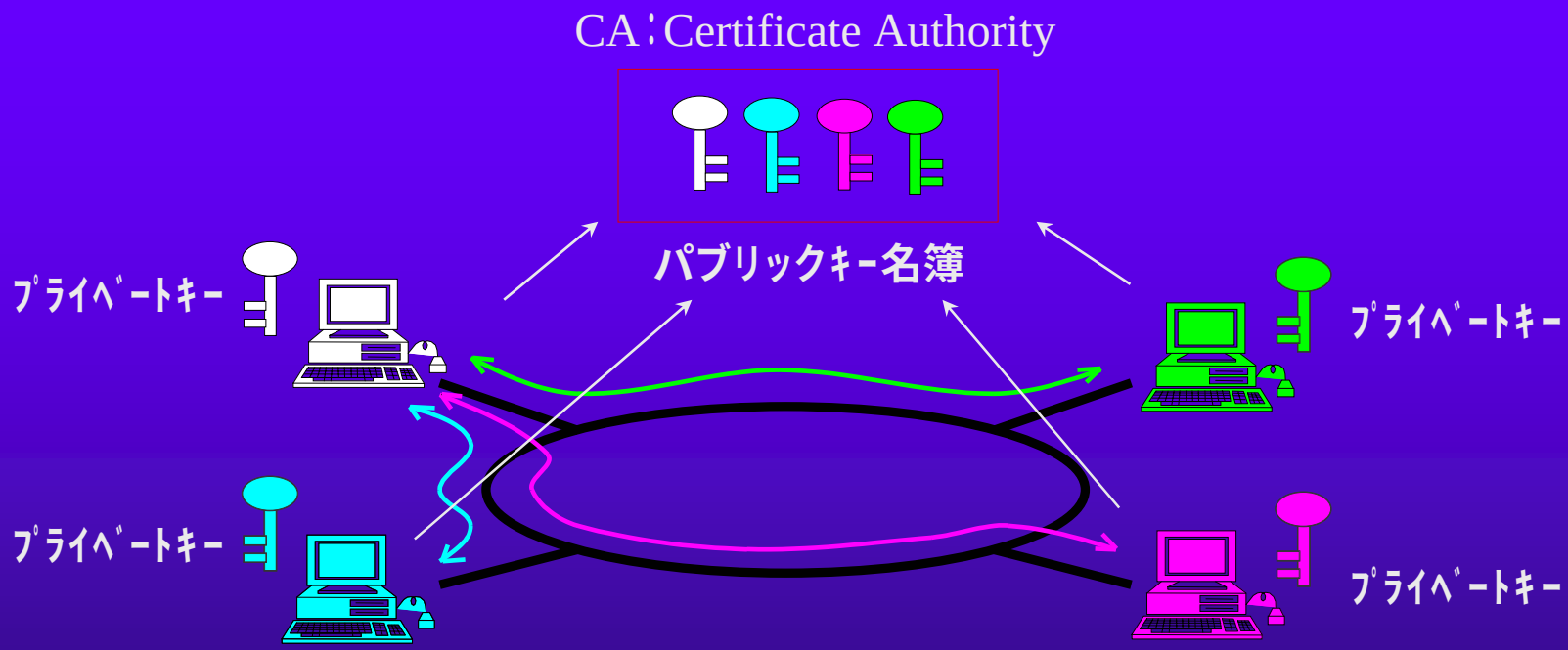
- 暗号化鍵と復号鍵が異なっている（各人がペアで用いる）
- 暗号化鍵の方は公開しても安全性が保たれる

ディジタル署名（電子署名）

- 署名を生成できるのは Private Key を持っている A だけ
- だれもが A の署名の正当性を確認することができる
- ネットワーク暗号における最も重要な機能

オープンネットワークでの暗号モデル

PKI (Public Key Infrastructure)



- 各ユーザーは自分のプライベートキーだけを管理すればよい
- 送信相手のパブリックキーはＣＡの名簿を参照して得る
- メッセージは共通鍵暗号で暗号化し、その鍵を公開鍵暗号で暗号化

公開鍵暗号の安全性の根拠

1．素因数分解問題の困難性　⇒ RSA暗号
2．離散対数問題の困難性　　⇒ ElGamal暗号

- 現在安全とされている公開鍵暗号の安全性の根拠はこの２つのうちの何れか
- このほかの数学的原理に基づく公開鍵暗号はほとんど解読されている
- これらの暗号は秘密鍵暗号に比べ低速

素因数分解型ーRSA初期設定

鍵生成と配布

・ユーザごとに独立に素数 p と素数 q を生成し
n = p×q を計算する。

・公開鍵 (ﾊﾟﾌﾞﾘｯｸｷｰ) e と秘密鍵 (ﾌﾟﾗｲﾍﾞｰﾄｷｰ)
d を次の式が成り立つように一組決める。

$$e \times d = 1 \pmod{(p-1)(q-1)}$$

・e, n が公開情報、p, q, d が秘密情報

・e はシステムパラメータ (例:65537) として
共通化することも多い

素因数分解型ーRSA暗号

暗号化

・暗号文Cは平文Mから次の式で計算する

$$C = M^e \pmod n$$

復号化

・平文Mは暗号文Cから次の式で計算する

$$M = C^d \pmod n$$

・通常 e は小さい値なので暗号化は高速,復号は低速

・ p, q はなくても復号は可能だが使うと高速化可能

素因数分解型ーRSA署名

署名生成

・署名Cは平文Mから次の式で計算する

$$C = \mathrm{Hash}(M)^d \pmod n$$

署名検証

・署名Cの検証は次の2式を比較する

$$\mathrm{Hash}(M) \text{ と } C^e \pmod n$$

・通常 e は小さい値なので検証は高速,生成は低速

・ p, q はなくても生成は可能だが使うと高速化可能

MISTY

1995年に設計された64ビットブロック暗号

- 差分解読法や線形解読法に対する安全性が数学的に保証できる

あらゆるプラットフォームで高速性を実現

- ＩＣ カードから高性能ワークステーションまであらゆるプラットフォームで高速性を実現する
- ソフトウエアだけでなくハードウエアでも充分な高速化が可能な構造を設計する

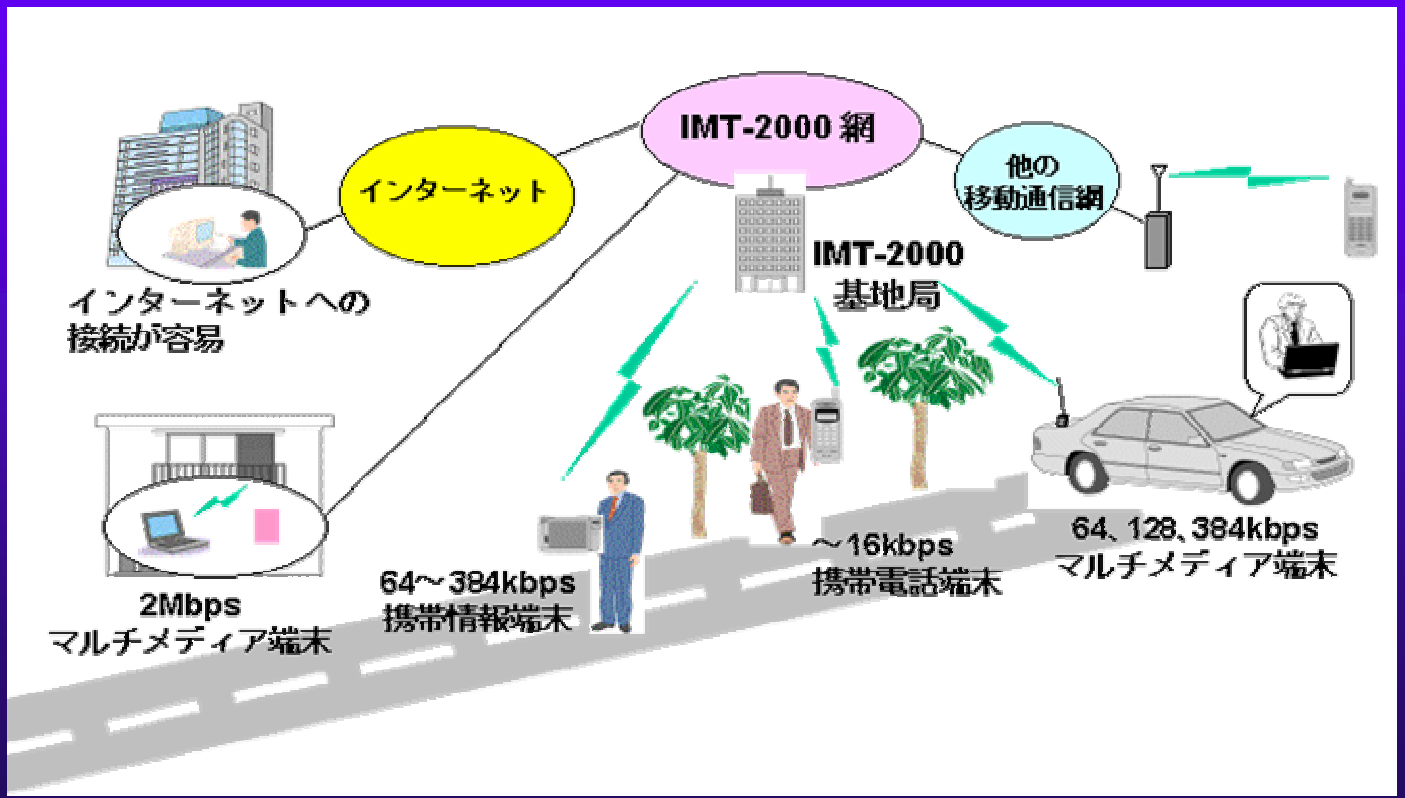
（当時はソフトウエア向け暗号全盛時代だった）

次世代（第三世代）移動通信

第三世代移動通信システムが目指すサービスの主な特徴は、以下のとおり。

- グローバルサービスの実現（様々な利用形態、地域を超え利用可能）
- マルチメディア通信サービスの提供（インターネットとの高い親和性）
- 固定網と同等な高品質なサービスの提供
- 高い周波数利用効率の実現（既存システムと同等以上の周波数利用効率）

（平成11年9月 電気通信技術審議会次世代移動通信方式委員会報告より）



Structure of 3GPP（'98.12～)

3GPP: third generation partnership project

3GPP = ARIB（日） CWTS（中）
ETSI（欧） T1（米）
TTA（韓） TTC（日）

- CN (Core Network)
- RAN (Radio Access Network)
- SA (Services and System Aspects)
  - WG1
  - WG2
  - WG3 (security)
  - WG4
  - WG5
- T (Terminal)

(http://www.3gpp.org)

Scope of 3G Security Standards

- Confidentiality（秘匿）
  - メッセージ暗号化により情報を保護
- Integrity（完全性）
  - メッセージ認証子により改ざん防止
- Authentication（認証）は標準化の範囲外
  - オペレータが独自に決定
- Confidentiality と Integrity メカニズムに共通に含まれる暗号アルゴリズムがKASUMI

History of KASUMI

- SA-WG3 が SAGE に 3G 暗号設計依頼 (99-春)
- SAGE で MISTY ベースでの開発を決定
  MISTY 開発者を暗号設計作業に招請 (99-7)
- SAGE での開発完了。中核となるアルゴリズムを
  KASUMIと命名 (99-11)
- 外部研究者者に安全性評価を依頼
  充分安全であるとの評価結果 (99-11,12)
- SAGE は SA-WG3 に対し作業完了を報告 (99-12)
- 3GPP が KASUMI をW-CDMA 暗号に正式採用 (00-3)

SAGE (Special Algorithm Group of Experts) :
ETSI 傘下の暗号専門家グループ、GSM 暗号を設計

Why MISTY ?

- **3G 暗号に対する要求条件**
  - １０年以上の利用に耐える高い安全性
    - 差分解読法や線形解読法に対する証明可能安全性
    - 国際的に知名度がありしかも利用実績がある
  - ハードウエアで充分小型（< 10Kゲート）
    - ハードウエアで6Kゲートのものがすでに開発済み
    - 安全でしかも10Kゲート以下で実現可能な暗号は極めて少ない

本標準化の意義

- “Public Confidence” を得るための周到なプロセス
  - 多国籍専門家集団による開発
  - 実績のある暗号をもとに開発
  - 中立的な外部研究者に安全性評価を委託
- 国産暗号技術が唯一の国際標準となるのは日本の暗号史上はじめて
- 世界で最も広く利用される暗号へ

ISO9979 暗号登録制度

- ISOにおいてDES の標準化失敗をうけて成立
- どんな暗号アルゴリズムも登録可能
- アルゴリズムを公開する必要もない
- 国内での登録申請は IPA が実施
- 安全性などの保証は一切ない
- 登録番号を交付されることにﾋﾞｼﾞﾈｽ上意義
- 最近、再度標準化を行う方向で進んでいる

ISO 登録暗号一覧 (2000年12月)

B-CRYPT	BT(UK)	1992
IDEA	Ascom(CH)	1993
LUC	LUC(NZ)	1994
DES	NCS(US)	1994
CDMF	IBM(US)	1994
Skipjack	NSA(US)	1994
RC4	RSADSI(US)	1994
RC2	RSADSI(US)	1994
MULTI2	Hitachi(JP)	1994
FEAL	NTT(JP)	1994
BARAS	ETSI(FR)	1995
SXAL/MBAL	Laurel Intelligent Systems (JP)	1995
MISTY1	Mitsubishi Electric(JP)	1996
ENCRiP	NEC(JP)	199
ACR	SAGEM(FR)	199
FWZ1	Check Point Software(IL)	1997
SPEAM1	Matsushita (JP)	199
ELCURVE	Hitachi (JP)	199
CIPHERUNICORN-E	NEC(JP)	1998
M8	Hitachi (JP)	199
GCC	International Information Science Institute (JP)	2000
TRIPLO	Toshiba (JP)	2000
FSAngo	Fuji Soft ABC (JP)	2000

ISO/IEC JTC1/SC27暗号標準化

- ９９年末に再び暗号の標準化に方向転換
- 公開されたアルゴリズムに限定
- 各国の国内委員会に候補提案を要請
- 共通鍵暗号とともに公開鍵暗号も標準化の対象
- 早ければ２００３年に標準化される可能性
- ＩＳＯは国（地域）が一票を投じて決定する

NESSIE プロジェクト (1/3)

- 欧州委員会が行なう欧州暗号標準化計画
  New European Schemes for Signatures, Integrity, and Encryption
- ２００２年末までの３年間のプロジェクト
- ＡＥＳと同じく公募を行なったのち選考する
- 専門家からなるボードメンバーが中心になる
- 選考方法などの詳細は現時点では未定
- ボードメンバーも有力な投稿者
- http://cryptonessie.org/

NESSIE プロジェクト (2/3)

- **NESSIEの計画**

2000年1月	NESSIEプロジェクト開始
2000年3月	公募要項公開
2000年9月	公募締め切り
2000年11月13,14日	第1回 NESSIE会議(ベルギー)
2001年9月12,13日	第2回 NESSIE会議 (イギリス)
2001年10月	第1次選考
2002年10月	第3回 NESSIE会議
2002年12月	最終選考

NESSIE 応募暗号一覧

公開鍵 (守秘)	ACE	IBM	共通鍵 (ストリーム)	BMGL	Hastard 他	Leviathan	Cisco
	ECIES	Certicom		LILI-128	Dawson 他	SOBER-t16	Qualcomm
	EPOC-1-2-3	NTT		SNOW	Johansson他	SOBER-t32	Qualcomm
	PSEC-1-2-3	NTT	共通鍵 (64ビットブロック)	CS-Cipher	CS Communication & Systems		
	RSA-OAEP	RSA		Khazad	Baretto, Rijmen		
公開鍵 (認証)	GPS	France Telecom		MISTY1	三菱電機	Nimbus	Machado
公開鍵 (署名)	ACE	IBM		Hierocrypt-L1	東芝	IDEA	Mediacryp
	ECDSA	Certicom	共通鍵 (128ビットブロック)	Anibus		Baretto, Rijmen	
	ESIGN	NTT		Caemellia		NTT, 三菱電機	
	FLASH	BULL CP8		Grand Cru		Borst	
	QUARTZ	BULL CP8		Noekeon		Daemen 他	
	SFLASH	BULL CP8		Q		McBride	
	RSA-PSS	RSA		SC2000		富士通	
ハッシュ関数	Whirlpool	Baretto,Rijmen		Hierocrypt-3		東芝	
メッセージ認証	Two-Track-MAC	Boer, Rompay	共通鍵 (160ビット)	SHACAL		Gemplus	
	UMAC	Rogaway 他	共通鍵 (複数ビット)	RC6	RSA	NUSH	LAN Cryp
				SAFER++	Cylink		

NESSIE 第1次選考結果

公開鍵 (守秘)	ACE (*)	IBM	共通鍵 (ストリーム)	BMGL	Hastard 他		
	ECIES	Certicom				SOBER-t16	Qualcomm
	EPOC-2 (*)	NTT		SNOW	Johansson他	SOBER-t32	Qualcomm
	PSEC-2 (*)	NTT	共通鍵 (64ビットブロック)				
	RSA-OAEP (*)	RSA		Khazad	Baretto, Rijmen		
公開鍵 (認証)	GPS	France Telecom		MISTY1	三菱電機		
公開鍵 (署名)						IDEA	Mediacryp
	ECDSA	Certicom	共通鍵 (128ビットブロック)				
	ESIGN (*)	NTT		Caemellia		NTT, 三菱電機	
	QUARTZ	BULL CP8					
	SFLASH	BULL CP8					
	RSA-PSS	RSA					
ハッシュ関数	Whirlpool	Baretto,Rijmen					
メッセージ認証	Two-Track-MAC	Boer, Rompay	共通鍵 (160ビット)	SHACAL		Gemplus	
	UMAC	Rogaway 他	共通鍵 (複数ビット)	RC6	RSA		
(*) はアルゴリズムの若干の変更があったもの				SAFER++	Cylink		

NESSIE プロジェクト (3/3)

- NESSIEの最終目標は産学の「コンセンサス」
  - ISO 等の標準化活動へのはたらきかけ
- 選考方法や選定アルゴリズム数は未定
  - 必ずしも1つに絞り込むことが目標ではない
- IPR (Intellectual Property Rights) Jungle
  - NESSIE は応募アルゴリズムの IPR に対する強制力をもたない
- 選考結果は大きな影響力をもつ可能性
  - 幅広い対象、超一流の主催者グループ、Industrial board との協調

国内における暗号標準化活動
暗号技術評価委員会 (1/3)

- CRYPTREC（Cryptography Research and Evaluation Committee）
- 2003年度の電子政府のセキュリティ基盤
- 暗号アルゴリズムを公募し選定する
- 専門的観点から評価しリストアップする
- 各省庁が暗号を利用する際の参考とする
- 2000年度は IPA の事業として実施
  (http://www.ipa.go.jp/security/)

国内における暗号標準化活動
暗号技術評価委員会 (2/3)

2000年度活動内容

暗号アルゴリズムの募集

共通鍵暗号、公開鍵暗号、ハッシュ関数、乱数生成法等

第1次スクリーニング評価

CRYPTREC 委員による書面審査

第2次詳細評価

内外の研究者に安全性・性能評価を委託

最終報告書作成・公開

http://www.ipa.go.jp/security/enc/CRYPTREC

国内における暗号標準化活動
暗号技術評価委員会 (3/3)

2001年度活動内容

総務省（TAO），経済産業省（IPA）の共同開催

暗号アルゴリズムの募集と評価

昨年度すでに評価したものについては、継続した詳細評価を実施するか、「監視対象」として登録

その他のアクティビティ

SSLプロトコルの評価、電子政府暗号の要件調査

最終報告書作成･公開

http://www.ipa.go.jp/security/enc/CRYPTREC

2001年度評価対象暗号一覧

公開鍵（署名）	ESIGN	NTT	共通鍵（ストリーム）	MULTI-S01	日立製作所
	RSA PKCS#1 1.5	ー		MUGI (*)	日立製作所
	RSA-PSS	RSALAB	共通鍵（64ビットブロック）	CIPHERUNICORN-E	日本電気
	DSA	ー		*Hierocrypt-L1*	東芝
	ECDSA	ー		*MISTY1*	三菱電機
	ECDSA in SEC1	富士通/Certicom		*TripleDES*	ー
公開鍵（守秘）	OK-ECDSA(*)	日立製作所	共通鍵（128ビットブロック）	*Camellia*	NTT/三菱電機
	EPOC-2	NTT		CIPHERUNICORN-A	日本電気
	HIME-R (*)	日立製作所		*RC6*	東芝
	RSA-OAEP	RSALAB		*SC2000*	RSALAB
	ECIES in SEC1	富士通/Certicom		*Rijndael*	富士通
	NTRU (*)	NTT		AES	ー
公開鍵（鍵共有）	*DH*	ー	ハッシュ関数	SHA-256,384,512	ー
	ECDH in SEC1	富士通/Certicom		*RIPEMD-160*	ー
	OK-ECDH (*)	日立製作所		*SHA-1*	ー
	PSEC-KEM (*)	NTT	擬似乱数生成法	*PRNG based on SHA1*	ー

斜字体は「監視状態の暗号」、(*) はスクリーニング対象
その他は詳細評価対象

暗号と政治 (1/2)

- 暗号の輸出規制
  - 多くの国で暗号の輸出は規制されている
    - 暗号は兵器と同じ扱いを受けるのが原則
    - 徐々に緩和の方向 (国際情勢に大きく依存)
  - ワッセナーアレンジメントに基づく国際協調
    - 旧ココムにかわる武器輸出管理体制
    - 1996年1月から。133カ国が参加
  - 国内関連法令
    - 輸出貿易管理令、外国為替令
    - 例外: 弱い暗号 (共通鍵56ビット以下、RSA512)
      金融・放送・携帯電話など規制外

暗号と政治 (2/2)

- Key Escrow (鍵寄託)
  - 米国政府の Capstone 計画の一環
  - 合法的盗聴を可能にするメカニズム
  - Clipper Chip への政治的･技術的批判
- Key Recovery (鍵回復)
  - Trusted Third Party による分散管理
  - 輸出規制回避の一方策の側面
  - Lost Key 回復は現実のシステム運用で必要

暗号技術の今後と課題

- 電子社会の見えざるインフラとして普及
  - 暗号なくしてディジタル通信なし
  - 世界中で標準化が行われている
  - プライバシー情報はICカードに格納される時代に
- 暗号技術の将来はバラ色か？
  - 暗号技術のオープン化はプライバシー保護と
    犯罪抑止の両立の難しさを顕在化させた
    ⇒ 解けない暗号は犯罪捜査への脅威
  - 暗号利用に関する何らかの制限は必要か？
    暗号解読研究の公表は制限されるべきではないか？

文献紹介

［入門書］

太田和夫他：情報セキュリティの科学ーマジックプロトコルへの招待
講談社 ブルーバックス (1995)

辻井重男 ：暗号 ーポストモダンの情報セキュリティー
講談社 選書メチエ73 (1996)

B.Schneier：**Applied Cryptography (second edition)**
John Wiley & Sons (1996)

岡本龍明：図解 暗号と情報セキュリティ 日経BP社 (1998)

［中級向］

岡本龍明他：現代暗号
産業図書 シリーズ／情報科学の数学 (1997)

A.Menezes,P.C.Oorschot,S.A.Vanstone：
Handbook of Applied Cryptography, CRC Press (1997)